

# PRIVACY POLICY

## Table of Contents

1. Purpose and Status of this Privacy Notice
2. Controller Identity and Privacy Contact
3. Scope of this Notice
4. Relationship with Other Terms and Layered Notices
5. Data-Protection Roles and Responsibility Allocation
6. Core Data-Protection Principles
7. Definitions
8. Categories of Data Subjects
9. Overview of Personal Data We Process
10. Account, Identity, Contact and Profile Data
11. Adult Eligibility, Age Assurance and Verification Data
12. Payment, Subscription, Wallet and Entitlement Data
13. Device, Network, Usage and Security Data
14. Communications, Chat, Prompts and Interaction Data
15. AI Processing, Conversation Memory and Personalization Data
16. Content, Media, Uploads and Generated Outputs
17. Hosted Client, Authorized User and Business Dashboard Data
18. Character Creation, ComfyUI, LoRA, Chatbot and Project Data
19. Revenue Share, Commission, Statements, Payout and Tax Data
20. Support, Moderation, Safety, Complaints and Legal Data
21. Analytics, Attribution, Communications and Marketing Data
22. Special-Category and Adult-Context Data
23. Sources of Personal Data
24. Purposes of Processing
25. Lawful Bases under GDPR
26. Detailed Purpose and Lawful-Basis Matrix
27. Consent and Explicit Consent
28. Legitimate Interests
29. Contract, Legal Obligation, Vital Interests and Legal Claims
30. Data Minimisation, Accuracy, Purpose Limitation and Privacy by Design
31. Minors and Data We Do Not Intentionally Seek
32. Recipient and Disclosure Principles
33. Categories of Recipients
34. Processors and Service Providers
35. Payment, Banking, Billing and Fraud Providers
36. Hosting, CDN, Storage and Infrastructure Providers
37. AI, Model, Automation and Content-Generation Providers
38. Age Assurance, Identity, KYC and Verification Providers
39. Analytics, Support, Communications and Marketing Providers
40. Professional Advisers, Corporate Transactions and Legal Recipients
41. Law Enforcement, Regulators, Safety and Rights Protection
42. User-Directed, Public and Interactive Disclosures

43. Hosted Client and Authorized User Access
44. Hosted Client Segregation, Confidentiality and Permitted Use
45. Data Processing Agreements and Role Allocation
46. Subprocessor Governance and Vendor Due Diligence
47. International Operations and Cross-Border Access
48. EU/EEA Adequacy Decisions and Recognised Destinations
49. EU Standard Contractual Clauses, Transfer Assessments and Supplementary Measures
50. Transfers to the United States
51. Transfers to Canada
52. Transfers to Israel
53. United Kingdom, Switzerland and Other Transfer Frameworks
54. Onward Transfers and Government Access Requests
55. Data Location, Remote Support and Localization
56. AI Inputs, Outputs, Memory, Embeddings and Vector Stores
57. AI Training, Fine-Tuning and Product Improvement
58. Hosted Client AI Projects, LoRA and Character Assets
59. Automated Moderation, Recommendations and Risk Scoring
60. Solely Automated Decisions and Human Review
61. Cookies and Similar Technologies Overview
62. Strictly Necessary and Functional Technologies
63. Analytics, Attribution, Advertising and Social Technologies
64. Consent Management, Browser Signals and Electronic Marketing
65. Security Governance and Confidentiality
66. Identity, Authentication, Access Control and Dashboard Security
67. Encryption, Pseudonymisation, Segregation and Key Management
68. Monitoring, Logging, Testing, Vulnerability and Supplier Security
69. Security Incidents, Breach Assessment and Business Continuity
70. Retention Principles
71. Retention Schedule - Accounts, Chat, AI and Content
72. Retention Schedule - Payments, KYC, Hosted Client and Support Data
73. Deletion, Anonymisation, Backups, Legal Holds and Derived Data
74. Aggregated, De-identified and Statistical Data
75. United States, Canada, Israel and Other Local Privacy Overlays
76. Sale, Sharing, Targeted Advertising and Sensitive Data
77. How to Submit a Privacy Rights Request
78. Identity, Account-Control and Authority Verification
79. Authorized Agents, Representatives and Rights on Behalf of Others
80. Response Times, Format, Fees and Communication
81. Right to Information and Transparency
82. Right of Access and Copies
83. Right to Rectification and Completion
84. Right to Erasure and Account Deletion
85. Erasure Exceptions, Legal Retention and Suppression Records
86. Right to Restriction of Processing
87. Right to Data Portability
88. Right to Object and Direct-Marketing Objections
89. Withdrawal of Consent and Explicit Consent
90. Adult-Context, Special-Category and Sensitive-Data Controls
91. Automated Decisions, Profiling and Human Review
92. AI Inputs, Outputs, Chat Memory, Embeddings and Derived Data Rights

- 93. Rights Concerning Hosted Clients, Model Accounts and Dashboards
- 94. Processor, Subprocessor and Recipient Cooperation
- 95. Content, Media, Depicted Persons and Privacy Complaints
- 96. United States State Privacy Rights
- 97. Canadian Privacy Rights
- 98. Israeli Privacy Rights
- 99. United Kingdom, Switzerland and Other Local Rights
- 100. Non-Discrimination, Service Consequences and Financial Incentives
- 101. Privacy Questions, Internal Complaints and Appeals
- 102. Supervisory Authorities and Regulatory Complaints
- 103. Judicial Remedies, Representation and Compensation
- 104. Communications Following a Personal Data Breach
- 105. Minors, Underage Data and Protective Deletion
- 106. Changes to this Privacy Policy and New Processing
- 107. Controller, Privacy, DPO and Service Contacts

## **1. Purpose and Status of this Privacy Notice**

**1.1** This Privacy Policy and GDPR Notice explains how Peachcream SRL, operating the CreamyPeach platform, collects, uses, generates, infers, receives, discloses and otherwise processes Personal Data in connection with its adult-only digital services and related business activities.

**1.2** This notice applies only to Personal Data. Information relating solely to a legal person is not Personal Data under the GDPR, but information about directors, beneficial owners, employees, contractors, sole traders, Authorized Users and other identifiable individuals is covered.

**1.3** Where a feature presents a shorter or more specific privacy notice at the point of collection, that notice supplements this document for the relevant processing. It does not reduce any mandatory right.

**1.4** The descriptions in this notice use “may” because the exact data collected depends on the individual’s role, the services used, the jurisdiction, risk signals, product configuration and the applicable Hosted Client arrangement.

## **2. Controller Identity and Privacy Contact**

**2.1** The principal controller for the core CreamyPeach platform is Peachcream SRL, operating the CreamyPeach brand and the website [creamypeach.com](https://creamypeach.com).

**2.2** The company registration identifier currently supplied for Peachcream SRL is ROONRC.J2026041854006. The registered office currently supplied is Soseaua Iancului nr. 53, Bucharest, Romania. The company tax identification number and VAT status must be inserted and verified before publication.

**2.3** Privacy questions and Data Subject requests may be sent to [privacy@creamypeach.com](mailto:privacy@creamypeach.com). General support may be contacted at [support@creamypeach.com](mailto:support@creamypeach.com), billing matters at [billing@creamypeach.com](mailto:billing@creamypeach.com), security reports at [security@creamypeach.com](mailto:security@creamypeach.com) and formal legal notices at [legal@creamypeach.com](mailto:legal@creamypeach.com), subject to any updated contact method published on the Website.

**2.4** Peachcream SRL is established in the European Union and therefore does not require an Article 27 EU representative for its own establishment. If a Data Protection Officer is appointed or becomes legally required, the DPO’s contact details will be published in the final policy.

**2.5** Before acting on a privacy request, CreamyPeach may take proportionate steps to verify identity, account control or authority, while avoiding collection of more verification information than reasonably necessary.

## **3. Scope of this Notice**

**3.1** This notice applies to visitors to CreamyPeach web properties; persons who pass through age gates; registered users; subscribers; purchasers; wallet users; users of chat, PPV, paid messages, tips, generated media and support tools; and persons who submit reports, complaints, legal notices or rights requests.

**3.2** It also applies to applicants for the Hosted Client Program; Hosted Clients; natural persons behind or connected with Hosted Clients; Authorized Users; beneficial owners; directors; employees; contractors; advisers; payout recipients; tax contacts; and persons using Business Dashboards or Model Accounts.

**3.3** It covers personal data contained in Client Materials, reference files, character-development datasets, ComfyUI workflows, LoRA training inputs, chatbot personality specifications, prompts, conversation configurations, content packages, rights documentation and other project materials submitted for One-Time Services.

**3.4** It also applies to rights holders, persons depicted or allegedly depicted in content, complainants, witnesses, reporters, security researchers, service-provider contacts, payment disputes, law-enforcement contacts and regulatory communications.

**3.5** This notice does not apply to third-party websites or services that determine their own processing purposes. Their privacy notices apply to their independent processing.

## **4. Relationship with Other Terms and Layered Notices**

**4.1** This notice should be read with the CreamyPeach Terms and Conditions, Cookie Policy, Billing and Wallet Policy, Refund Policy, Acceptable Use Policy, Community Guidelines, age-verification notices, checkout disclosures and any Hosted Client Order Form, Statement of Work or Data Processing Addendum.

**4.2** The Terms govern contractual use of the Platform. This notice governs Personal Data processing. If a contractual term conflicts with mandatory Data Protection Law, the mandatory privacy rule prevails for the Personal Data issue.

**4.3** A point-of-collection notice may provide more specific information about age verification, biometric or facial analysis, payment processing, a new AI feature, optional personalization, marketing consent, a hosted-client workflow or another specialized activity.

**4.4** Where consent is requested, the consent text and user-interface choice form part of the transparency information for that processing and must be retained in Version Records.

**4.5** Hosted Clients must not replace or contradict CreamyPeach privacy notices within the Platform. Any independent notice supplied by a Hosted Client must clearly identify the Hosted Client, its purpose and its own contact details.

## **5. Data-Protection Roles and Responsibility Allocation**

**5.1** Peachcream SRL acts as controller for the core Platform, including account administration, eligibility controls, subscriptions, wallet records, content entitlements, payment reconciliation, AI-assisted service delivery, personalization configured by CreamyPeach, moderation, fraud prevention, security, support, complaints, legal compliance and platform analytics.

**5.2** Payment processors, banks, card networks, age-verification providers and other vendors may act as processors, independent controllers or a combination of roles depending on their services and legal duties

**5.3** A Hosted Client is generally a separate controller for Personal Data it independently supplies, collects or uses for its own business purposes, including its Authorized Users, personnel, independent marketing, rights-clearance records and instructions concerning Client Materials.

**5.4** A Hosted Client does not automatically become a controller of all End-User Data merely because it receives dashboard access. CreamyPeach will limit access to data reasonably necessary for the configured role and may withhold payment credentials, sensitive security signals, unrelated conversations and data belonging to other clients.

**5.5** If CreamyPeach and a Hosted Client jointly determine the purposes and essential means of a particular processing activity, the parties will document their respective responsibilities as required by Article 26 GDPR. Joint controllership will not be assumed merely because both parties have commercial interests.

**5.6** If CreamyPeach processes Personal Data solely on documented instructions from a Hosted Client, or a Hosted Client processes data solely on CreamyPeach instructions, the parties will use an Article 28-compliant Data Processing Addendum where required.

**5.7** CreamyPeach remains an independent controller for its own billing, accounting, fraud prevention, security, legal compliance, dispute handling, service improvement and legal-claims purposes, even where another processing activity is performed as a processor.

## **6. Core Data-Protection Principles**

**6.1** CreamyPeach intends to process Personal Data lawfully, fairly and transparently, for specified and legitimate purposes, and not in a manner incompatible with those purposes.

**6.2** CreamyPeach will seek to limit Personal Data to what is adequate, relevant and reasonably necessary for the stated purpose, taking account of the risks created by adult-context data, private communications, payment activity and AI-assisted services.

**6.3** Reasonable steps will be taken to keep Personal Data accurate and to correct or delete inaccurate data where appropriate and legally permitted.

**6.4** Personal Data will be retained no longer than necessary for the relevant purpose, subject to legal, accounting, tax, fraud, chargeback, safety, rights, security and legal-hold requirements.

**6.5** CreamyPeach will apply proportionate technical and organizational measures designed to protect confidentiality, integrity, availability and resilience.

**6.6** CreamyPeach will maintain documentation and controls intended to demonstrate accountability, including records of processing, lawful-basis assessments, consent records, vendor arrangements, privacy impact assessments where required and role-allocation documents for Hosted Clients.

## 7. Definitions

**7.1** The following definitions apply to this Privacy Policy unless the context requires otherwise. Terms defined in the CreamyPeach Terms retain compatible meanings.

**Account Data:** information associated with creating, authenticating, configuring, securing or administering an Account.

**Adult-Context Data:** Personal Data arising from or connected with use of an adult-oriented service, including content interests, interactions and purchase patterns that may carry heightened confidentiality risks.

**Age Assurance:** methods used to estimate, confirm or support a conclusion that a person has reached the required age, which may include age gates, declarations, payment checks, document checks or third-party services.

**Age Verification Data:** information processed to verify or support verification of age or identity, including verification status, date, method, provider reference and, where specifically implemented, identity documents, facial images or related results.

**AI Input:** a prompt, message, instruction, file, image, preference, memory item, metadata or other information supplied to or used by an AI System.

**AI Interaction Data:** data generated by, supplied to or observed during interactions with AI-assisted chat, recommendation, generation, moderation or personalization features.

**AI Output:** text, media, labels, rankings, summaries, classifications, risk signals, recommendations or other results generated or assisted by an AI System.

**Authorized User:** an individual authorized by a Hosted Client to access a Business Dashboard, Model Account, project workspace or related business feature.

**Biometric Data:** Personal Data resulting from specific technical processing relating to physical, physiological or behavioural characteristics that allows or confirms unique identification, as defined by applicable law.

**Business Dashboard:** a role-based interface through which a Hosted Client may access permitted model, project, analytics, revenue, statement, payout, support or compliance information.

**Character Assets:** reference images, identity specifications, style guides, LoRA files, sample outputs, prompts and other assets used to create or operate a Hosted Model or Virtual Creator.

**Chat Memory:** stored summaries, preferences, facts, interaction history or other information used to maintain continuity or personalize later interactions.

**Client Materials:** content, personal data, instructions, reference files, brand assets, rights records and other materials provided by or for a Hosted Client.

**Commission Data:** records used to calculate CreamyPeach's platform commission and the Hosted Client share, including revenue, deductions, refunds, chargebacks, processor fees, taxes, adjustments and reserves.

**Consent:** a freely given, specific, informed and unambiguous indication of wishes expressed by a statement or clear affirmative action.

**Controller:** the person or entity that determines the purposes and means of processing Personal Data.

**Cookies and Similar Technologies:** cookies, SDKs, pixels, local storage, tags, identifiers and related technologies used for sessions, security, preferences, analytics or marketing.

**Data Protection Law:** the GDPR, Romanian implementing law, applicable ePrivacy rules and other privacy or data-protection laws that apply to a processing activity.

**Data Subject:** an identified or identifiable natural person to whom Personal Data relates.

**Device and Network Data:** IP address, device identifiers, browser information, operating system, session information, network data, approximate location and related technical signals.

**End User:** a visitor, account holder, subscriber, purchaser, wallet user, fan or other person using the customer-facing Platform.

**Explicit Consent:** consent expressed through an explicit statement or similarly clear action that satisfies Article 9 requirements where applicable.

**Hosted Client:** an external business customer approved to host, operate or commercialize one or more Hosted Models or receive related services on CreamyPeach.

**Hosted Model:** a creator-style profile, character, Virtual Creator or model hosted or operated under the Hosted Client Program.

**Inference:** a conclusion, prediction or classification derived from observed data, such as likely interests, preferences, fraud risk, content suitability or engagement probability.

**KYC Data:** identity, business, beneficial ownership, tax, sanctions, payout and verification information processed for onboarding or compliance.

**Lawful Basis:** a legal ground under Article 6 GDPR, together with an Article 9 condition where Special-Category Data is processed.

**Legitimate Interests Assessment:** a documented assessment of the purpose, necessity and balancing of interests, rights and safeguards for processing under Article 6(1)(f) GDPR.

**LoRA:** a low-rank adaptation file or technique used to adapt an AI model, which may be trained using reference images or other project data.

**Model Account:** a Platform account or operational profile associated with a Hosted Model or Virtual Creator.

**Payment Data:** transaction, billing, payment-method metadata, processor references, authorization results, receipt data, dispute data and related records; it does not ordinarily include full card numbers stored by CreamyPeach.

**Personal Data:** any information relating to an identified or identifiable natural person.

**Processing:** any operation performed on Personal Data, including collection, recording, organization, storage, adaptation, retrieval, consultation, use, disclosure, alignment, restriction, deletion or destruction.

**Processor:** a person or entity that processes Personal Data on behalf of a controller.

**Profiling:** automated processing used to evaluate or predict personal aspects such as preferences, interests, behaviour, reliability, spending patterns, risk or likely engagement.

**Prompt Data:** prompts, instructions, negative prompts, parameters, configuration data and related records used for AI chat or media generation.

**Pseudonymisation:** processing that separates Personal Data from direct identifiers so it cannot be attributed to a person without additional information kept separately.

**Revenue Share Data:** data concerning revenue attribution, commission, Hosted Client share, reserves, statements, payment status and payout calculations.

**Special-Category Data:** Personal Data covered by Article 9 GDPR, including data revealing health, sex life or sexual orientation, and Biometric Data used for unique identification.

**Transaction Data:** records of subscriptions, wallet top-ups, Credits, purchases, PPV unlocks, tips, paid messages, refunds, reversals, chargebacks and entitlements.

**User Content:** messages, prompts, uploads, profile information, reports, support submissions, images, audio, video and other content provided by an individual.

**Wallet Data:** balances, ledger entries, top-ups, deductions, promotional Credits, unlocks, refunds, reversals and adjustments.

7.2 References to examples are illustrative and do not limit a category where another item is materially similar.

## 8. Categories of Data Subjects

**8.1** CreamyPeach may process Personal Data relating to visitors, prospective users, registered users, subscribers, purchasers, wallet users, chat users, content viewers, support contacts and former users.

**8.2** CreamyPeach may process Personal Data relating to Hosted Client applicants, Hosted Clients, Authorized Users, directors, beneficial owners, sole traders, employees, contractors, advisers, representatives, payout recipients and tax contacts.

**8.3** CreamyPeach may process Personal Data relating to persons whose image, voice, likeness, identity, work or rights appear in Client Materials, Character Assets, complaints, copyright notices, non-consensual-content reports or other submissions.

**8.4** CreamyPeach may process Personal Data relating to complainants, reporters, witnesses, rights holders, security researchers, regulators, law-enforcement personnel, vendor contacts, professional advisers and other business contacts.

**8.5** A single person may fall into more than one category, and the same data item may be processed for different compatible purposes under different lawful bases.

## 9. Overview of Personal Data We Process

**9.1** Depending on the relationship and feature used, CreamyPeach may process Account Data, contact information, eligibility information, Age Verification Data, Payment Data, Transaction Data, Wallet Data, subscriptions, entitlements, communications, User Content, AI Interaction Data, Device and Network Data, support records, moderation data and legal records.



**9.2** For Hosted Clients, CreamyPeach may additionally process KYC Data, business-contact data, Authorized User data, Client Materials, Character Assets, project specifications, deliverables, Revenue Share Data, Commission Data, payout information, tax data, statements and Business Dashboard activity.

**9.3** CreamyPeach may create or derive operational data, including content classifications, entitlement records, Chat Memory, fraud scores, abuse signals, recommendations, moderation outcomes, risk flags, aggregated analytics and other Inferences.

**9.4** Some data may be sensitive because of the adult context even when it does not meet the legal definition of Special-Category Data. CreamyPeach will treat private adult-context interactions as confidential and apply heightened access controls appropriate to the risk.

**9.5** Not all data categories are mandatory. When data is required, the interface or contract should indicate whether it is needed to enter a contract, receive a service, comply with law or use a particular feature, and the consequence of not providing it.

## **10. Account, Identity, Contact and Profile Data**

**10.1** Account Data may include email address, username, password hash, account identifier, age declaration, country or region, language, time zone, consent choices, notification preferences, account status, profile settings and recovery information.

**10.2** Identity and contact data may include legal name, display name, postal address, telephone number, email address, date of birth where required, identity-document details, verification status and communications preferences.

**10.3** Profile data may include avatar, biography, interests, content preferences, followed models, blocked accounts, favourite content, subscription choices and other information a user chooses to add or that is necessary to configure the service.

**10.4** Authentication and account-control data may include password-reset records, multi-factor authentication status, verification events, login history, device/session history, security challenges and account-ownership evidence.

**10.5** CreamyPeach processes this data to create and administer Accounts, authenticate users, provide settings, communicate service information, resolve ownership disputes, prevent account abuse and satisfy contractual or legal obligations.

## **11. Adult Eligibility, Age Assurance and Verification Data**

**11.1** CreamyPeach may process an age declaration, date-of-birth confirmation, jurisdiction, age-gate response, verification status, verification date, method, provider reference and risk indicators to enforce adult-only access.

**11.2** Where enhanced age or identity verification is implemented, a provider may process an identity document, selfie, facial image, liveness result, document-validity information or other verification data. CreamyPeach should seek to receive only the minimum result and metadata necessary where the provider can retain raw data independently.

**11.3** If a verification method uses Biometric Data for unique identification, or otherwise processes Special-Category Data, the point-of-collection notice will identify the processing, controller roles, Article 9 condition, retention approach and available alternatives where required.

**11.4** Age-assurance and verification data may be used to grant or deny access, investigate suspected minor access, prevent repeated circumvention, satisfy processor or legal requirements and maintain evidence of compliance.

**11.5** CreamyPeach will not treat possession of a payment method as conclusive proof of age and may require additional checks where risk, law or processor requirements justify them.

**11.6** Hosted Clients and Authorized Users may also be required to provide age and identity verification, particularly where they can access adult content, model operations, payouts or sensitive business information.

## **12. Payment, Subscription, Wallet and Entitlement Data**

**12.1** Payment Data may include processor customer ID, transaction ID, authorization result, amount, currency, tax, billing country, billing descriptor, payment-method type, limited card metadata, receipt, refund status, chargeback information and processor fraud signals.

**12.2** CreamyPeach does not intend to store full payment card numbers on its own systems. Full payment credentials are expected to be handled by authorized payment processors or tokenization providers, subject to their own privacy and legal obligations.

**12.3** Subscription data may include plan, price, start date, renewal date, cancellation date, trial status, renewal history, failed-payment events, access status and related notices.

**12.4** Wallet Data may include purchased and promotional Credits, balance, top-ups, deductions, content unlocks, paid messages, tips, gifts, reversals, refunds, chargebacks, adjustments and restrictions.

**12.5** Entitlement data may include the content, model, message, feature or subscription area an Account is permitted to access, together with activation, delivery, revocation and expiration records.

**12.6** This data is used to perform transactions, provide access, maintain accounting records, respond to billing errors, prevent duplicate recovery, manage refunds and chargebacks, satisfy tax obligations and protect the integrity of the payment system.

## **13. Device, Network, Usage and Security Data**

**13.1** CreamyPeach may collect IP address, device identifiers, browser type, operating system, app or web version, language, time zone, session identifiers, cookie identifiers, approximate location, network or proxy signals, referrer, timestamps and technical logs.

**13.2** Usage data may include pages viewed, features used, searches, clicks, content impressions, media playback, chat events, purchases, unlocks, session duration, errors, performance data, navigation paths and interaction metadata.

**13.3** Security data may include login attempts, authentication events, credential-stuffing indicators, suspicious device changes, rate-limit events, malware or bot signals, token use, session anomalies, account-linkage signals and investigation results.

**13.4** Device, network and usage data may be used to provide the service, maintain sessions, remember settings, measure performance, troubleshoot, protect accounts, detect fraud, enforce restrictions, prevent scraping and support legal or chargeback evidence.

**13.5** Approximate location may be inferred from IP address, billing country, payment country or device settings. Precise geolocation will not be collected unless a feature requires it, a clear notice is provided and an appropriate lawful basis applies.

## **14. Communications, Chat, Prompts and Interaction Data**

**14.1** CreamyPeach may process messages, chat content, prompts, requests, attachments, media interactions, reactions, timestamps, delivery status, moderation flags, pricing events and conversation metadata.

**14.2** Chat and prompt data may include intimate or adult-context statements, preferences, fantasies, roleplay instructions and other information chosen by the user. Users should avoid providing unnecessary identity documents, financial information, health information, real-world addresses or third-party Personal Data in chat.

**14.3** Communications may be processed to deliver replies, generate or select media, maintain continuity, price or unlock content, moderate prohibited requests, detect abuse, provide support, investigate complaints and improve service quality.

**14.4** CreamyPeach may use automated filters, classifiers, keyword systems, risk rules and human review to identify illegal content, minors, non-consensual content, threats, fraud, exploitation, payment circumvention or other prohibited conduct.

**14.5** Hosted Clients or Authorized Users may receive access to limited model-output or interaction information only where configured for legitimate model operation, content approval, support, safety, analytics or revenue purposes. Access does not include an unrestricted right to extract or reuse End-User conversations.

**14.6** The final policy must identify whether and to what extent chat content is retained, used for model evaluation or training, reviewed by humans or disclosed to Hosted Clients.

## **15. AI Processing, Conversation Memory and Personalization Data**

**15.1** AI Inputs may include chat messages, prompts, profile preferences, selected model, previous interactions, purchased features, content history, safety context and technical parameters. AI Outputs may include messages, images, videos, captions, recommendations, classifications, moderation signals and summaries.

**15.2** CreamyPeach may create Chat Memory or preference profiles to maintain continuity, remember user-selected facts, adapt tone, recommend content, avoid repetition, identify spending state, manage relationship context and improve the requested interaction.

**15.3** The lawful basis for core AI processing is generally performance of the requested service or steps taken at the user's request. Legitimate interests may support safety, quality assurance, error detection, service improvement and non-intrusive personalization where the balancing test is satisfied.



**15.4** Optional personalization that is not necessary to provide the requested service will use consent where required. If personalization involves or infers Special-Category Data, CreamyPeach will obtain Explicit Consent or rely on another valid Article 9 condition before using that data for the sensitive purpose.

**15.5** CreamyPeach may use aggregated, statistical, pseudonymised or de-identified information to evaluate performance and improve systems. If identifiable conversations or media are to be used to train or fine-tune a model for a purpose beyond delivering and protecting the service, CreamyPeach will identify the purpose, lawful basis, recipients and available choices before that use.

**15.6** AI-derived Inferences may be inaccurate. CreamyPeach will provide correction, deletion, objection or opt-out mechanisms where required and will avoid treating sensitive Inferences as verified facts without appropriate confirmation.

## **16. Content, Media, Uploads and Generated Outputs**

**16.1** CreamyPeach may process uploaded images, video, audio, text, prompts, support attachments, profile materials, content metadata, watermarks, content hashes, rights information, consent records and generated outputs.

**16.2** Content metadata may include creation time, file type, file size, dimensions, model or workflow identifiers, prompt parameters, content classification, moderation status, publication status, access rights and revenue attribution.

**16.3** Content may be processed to generate, edit, transcode, store, publish, stream, watermark, moderate, classify, recommend, sell, unlock, investigate or remove media and related digital services.

**16.4** CreamyPeach may process face, voice, likeness or identity information where it appears in content. If such data relates to a real person, the submitting party must have an appropriate lawful basis, rights and consent, and CreamyPeach may require supporting records.

**16.5** Content involving suspected minors, non-consensual intimate content, impersonation or rights violations may be restricted, preserved and reviewed for safety, legal, evidentiary and enforcement purposes.

**16.6** Where generated outputs are associated with a Hosted Model rather than a real person, they may not constitute Personal Data by themselves; however, prompts, account data, identifiable references, operator activity and associated metadata may still be Personal Data.

## **17. Hosted Client, Authorized User and Business Dashboard Data**

**17.1** Hosted Client data may include business name, legal form, registration details, registered office, business email, telephone number, website, representatives, contracts, service selections, support history and commercial communications.

**17.2** For individuals connected with a Hosted Client, CreamyPeach may process name, role, employer, professional contact details, authority, signature, login credentials, multi-factor authentication status, device data, access logs and actions performed in the Business Dashboard or Model Account.

**17.3** Onboarding may require KYC Data, including identity documents, beneficial ownership, tax residence, tax identification, VAT status, sanctions information, payout account ownership and related verification evidence.

**17.4** Business Dashboard data may include Hosted Model status, content-production status, project orders, approvals, generated outputs, aggregate audience analytics, revenue, commission, deductions, reserves, statements, payout status, support cases and compliance notices.

**17.5** CreamyPeach processes this data to evaluate and onboard Hosted Clients, enter and perform contracts, secure role-based access, provide services, calculate fees and revenue share, prevent fraud, satisfy tax and regulatory duties, manage disputes and protect Platform users.

**17.6** Hosted Clients must not use dashboard data to identify, contact, profile or market to End Users outside the purposes and access permissions authorized by CreamyPeach and applicable Data Protection Law.

## **18. Character Creation, ComfyUI, LoRA, Chatbot and Project Data**

**18.1** One-Time Services may involve Client Materials such as reference images, videos, voice samples, names, biographies, brand assets, body and face specifications, style requirements, prompts, negative prompts, personality descriptions, conversation scripts, memory rules and sample outputs.

**18.2** Character-development and ComfyUI data may include workflows, node configurations, checkpoints, LoRA files, training datasets, captions, masks, control images, seed values, model versions, generation parameters, quality-review notes and delivery records.

**18.3** Chatbot-personality and automation data may include persona profiles, tone rules, prohibited topics, user-memory schemas, sales logic, spending state, response timing, content-selection rules, fallback messages and test conversations.

**18.4** Where Client Materials contain Personal Data, CreamyPeach will process them to scope, create, test, revise, deliver, host and support the contracted service, manage intellectual-property and consent risks, and maintain project records.

**18.5** The Hosted Client is responsible for providing lawful Client Materials and must not submit real-person likenesses, identity documents, voice samples, private communications or training data unless it has the authority, notices and consents required for the intended processing.

**18.6** An Order Form or Data Processing Addendum should specify whether CreamyPeach acts as controller or processor for project files, who may access them, permitted model training, retention after delivery, export rights, deletion, third-party tools and security requirements.

**18.7** CreamyPeach may retain limited project, rights, security and evidentiary records as an independent controller even after processor-held working files are returned or deleted, where necessary for legal claims, accounting, fraud prevention or compliance.

## **19. Revenue Share, Commission, Statements, Payout and Tax Data**

**19.1** Revenue Share Data may include model attribution, gross settled revenue, taxes, refunds, chargebacks, fraud losses, processor costs, credits, adjustments, reserves, Commissionable Revenue, the CreamyPeach commission, Hosted Client share and final payout amount.

**19.2** Payout data may include beneficiary name, bank or payment-account details, IBAN, payment provider, currency, payout schedule, threshold, status, failed-payment information and reconciliation records.

**19.3** Tax and reporting data may include tax residence, tax identification number, VAT number, business registration, beneficial ownership, reportable consideration and information required by accounting, anti-fraud, sanctions or platform-reporting regimes such as DAC7 where applicable.

**19.4** CreamyPeach processes this data to calculate and explain statements, collect hosting and project fees, apply the agreed 30 percent commission or another Order Form rate, pay the Hosted Client share, hold reserves, recover negative balances, reconcile processor records and satisfy legal obligations.

**19.5** Dashboard revenue figures may be provisional and may be corrected after refunds, chargebacks, processor reconciliation, tax adjustments, fraud review or error correction. Personal Data contained in statements will be limited to what is needed for the recipient and purpose.

**19.6** Payment and tax records may be shared with processors, banks, accountants, auditors, tax authorities and regulators, required by law.

## **20. Support, Moderation, Safety, Complaints and Legal Data**

**20.1** Support data may include tickets, emails, chat transcripts, screenshots, attachments, account identifiers, transaction references, troubleshooting details, identity-verification information and support outcomes.

**20.2** Moderation and safety data may include reports, flagged content, prompts, message excerpts, content hashes, classifier results, reviewer notes, reasons, warnings, appeals, prior violations, account links and evidence-preservation records.

**20.3** Fraud and payment-abuse data may include risk scores, device links, velocity patterns, payment tests, disputed transactions, chargeback narratives, delivery evidence, refund history and account restrictions.

**20.4** Legal and rights data may include copyright notices, non-consensual-content reports, consent disputes, identity claims, subpoenas, preservation requests, regulatory correspondence, court records and legal advice.

**20.5** CreamyPeach processes this data to answer requests, protect users, detect and prevent illegal or prohibited activity, enforce policies, provide reasons and appeals, defend claims, preserve evidence and comply with lawful requests.

**20.6** Where a report contains Special-Category Data or criminal-allegation information, access will be restricted and a specific legal condition will be identified where required.

## **21. Analytics, Attribution, Communications and Marketing Data**

**21.1** Analytics data may include page views, feature use, traffic source, campaign identifier, conversion events, aggregated audience segments, subscription and purchase funnels, model performance, retention and technical performance.

**21.2** Attribution data may include referral links, campaign codes, affiliate identifiers, social-media source, landing page, device category and related conversion records.

**21.3** Service communications may include account notices, receipts, security alerts, support replies, policy updates, renewal messages, payout notices and other non-promotional communications necessary for the relationship.

**21.4** Marketing data may include email address, marketing preferences, campaign engagement, audience selection, suppression status and consent records. Marketing will rely on consent where required and on legitimate interests only where applicable law permits and the individual's rights are respected.

**21.5** Hosted Client analytics should be aggregated or limited where possible. A Hosted Client will not receive unrestricted End-User identity or contact details merely to evaluate model performance.

## **22. Special-Category and Adult-Context Data**

**22.1** Use of an adult-oriented Platform, private messages, content preferences, custom requests and purchase patterns may reveal or allow Inferences about a person's sex life or sexual orientation, which are Special-Category Data under Article 9 GDPR when the legal threshold is met.

**22.2** Users may also voluntarily disclose health information, biometric information, religious or political views, ethnicity or other sensitive information in messages, prompts, support requests or uploaded content. CreamyPeach does not require such information for ordinary use and asks users not to provide it unless necessary for a specific supported purpose.

**22.3** CreamyPeach will not process Special-Category Data merely because it is technically available. A valid Article 9 condition must apply in addition to an Article 6 lawful basis.

**22.4** Where sensitive personalization is optional, CreamyPeach will normally rely on Explicit Consent. Refusing or withdrawing consent may disable that sensitive personalization without affecting unrelated services.

**22.5** Other Article 9 conditions may apply where processing is necessary to protect vital interests when consent cannot be obtained, establish, exercise or defend legal claims, process data manifestly made public by the Data Subject, or comply with a specific substantial-public-interest law. These grounds will be used narrowly.

**22.6** Biometric Data used for unique identification will not be processed without a specific Article 9 condition, clear notice, data-minimisation controls and appropriate security measures.

**22.7** CreamyPeach will not infer sensitive traits for unrelated advertising, eligibility or discriminatory treatment and will not treat fantasy or roleplay statements as verified facts about a user.

## **23. Sources of Personal Data**

**23.1** CreamyPeach receives Personal Data directly from individuals when they visit, register, verify age, purchase, subscribe, use Credits, chat, upload content, configure preferences, contact support, submit reports or exercise rights.

**23.2** CreamyPeach receives data from Hosted Clients and Authorized Users through applications, Order Forms, Client Materials, project files, dashboards, approvals, payout details, rights documents and instructions.

**23.3** CreamyPeach receives transaction, fraud, dispute and limited payment information from Payment Processors, banks, card networks, wallet providers, billing agents and fraud-prevention vendors.

**23.4** CreamyPeach may receive age, identity, sanctions, business, tax or verification results from verification providers, official registers, public databases, professional advisers and supporting documents.

**23.5** CreamyPeach automatically receives Device and Network Data, usage data, cookie data, security logs, entitlement events and AI-interaction metadata through use of the Platform.

**23.6** CreamyPeach may receive reports and information about a person from other users, rights holders, complainants, Hosted Clients, law enforcement, regulators, hosting providers and security researchers.

**23.7** CreamyPeach may receive referral or campaign information from social networks, affiliates, advertising partners or external websites where the individual follows a link or interacts with a campaign, subject to applicable consent requirements.

**23.8** Where data is obtained indirectly, CreamyPeach will provide Article 14 information where required unless a lawful exemption applies.

## **24. Purposes of Processing**

**24.1** CreamyPeach processes Personal Data to provide, personalize, administer and support the Website, Accounts, adult-only content, subscriptions, Wallet, Credits, PPV, paid chat, generated media, content entitlements and other requested Digital Services.

**24.2** CreamyPeach processes data to provide AI-assisted chat, recommendations, media generation, Chat Memory, content selection, quality controls and user-configured personalization.

**24.3** CreamyPeach processes data to verify adult eligibility, prevent minor access, detect exploitation and non-consensual content, moderate prohibited conduct, protect users and cooperate with appropriate authorities.

**24.4** CreamyPeach processes data to authenticate users, secure accounts, maintain availability, troubleshoot, prevent bots and scraping, detect fraud, investigate chargebacks and protect payment integrity.

**24.5** CreamyPeach processes data to enter and perform Hosted Client agreements, provide monthly hosting, Business Dashboards, Model Accounts, One-Time Services, character and ComfyUI work, LoRA training, chatbot-personality services and automation.

**24.6** CreamyPeach processes data to calculate fees, the 30 percent commission or agreed rate, Hosted Client share, statements, reserves, deductions, payouts, invoices, taxes and regulatory reports.

**24.7** CreamyPeach processes data to respond to support, billing, privacy, safety, copyright, content-removal and legal requests; provide reasons and appeals; preserve evidence; and establish, exercise or defend legal claims.

**24.8** CreamyPeach processes data to analyze service performance, understand feature use, prevent errors, develop and improve products, evaluate AI quality, conduct research with aggregated or pseudonymised data and plan business operations.

**24.9** CreamyPeach processes data to send service communications and, where lawful, marketing communications, promotions, product information and Hosted Client communications.

**24.10** CreamyPeach may process data for another compatible purpose or a new purpose only after assessing compatibility, identifying a lawful basis and providing any notice or consent required by law.

## 25. Lawful Bases under GDPR

**25.1** CreamyPeach relies on performance of a contract or steps requested before entering a contract where processing is objectively necessary to create an Account, provide purchased or requested services, deliver content, operate a Wallet, process a Hosted Client order, calculate revenue share or provide support connected with the contract.

**25.2** CreamyPeach relies on compliance with legal obligations where processing is required by tax, accounting, court, regulatory, sanctions, reporting, consumer, child-safety, payment or other applicable law.

**25.3** CreamyPeach relies on legitimate interests where it has a lawful and specific business, safety or security interest; the processing is necessary; and the individual's interests, rights and reasonable expectations do not override that interest.

**25.4** CreamyPeach relies on consent for optional processing where consent is the appropriate basis, including non-essential cookies, certain marketing, optional personalization and other features identified at the point of choice.

**25.5** CreamyPeach relies on Explicit Consent or another Article 9 condition when processing Special-Category Data.

**25.6** CreamyPeach may rely on vital interests in a genuine emergency involving a person's life or physical safety where consent cannot reasonably be obtained.

**25.7** Where processing is necessary to establish, exercise or defend legal claims, CreamyPeach may rely on legitimate interests and Article 9(2)(f) where Special-Category Data is involved.

**25.8** A lawful basis is assessed per purpose. CreamyPeach will not use "contract" or "legitimate interests" as a blanket justification for unrelated or unexpected processing.

## 26. Detailed Purpose and Lawful-Basis Matrix

**26.1** The matrix below identifies the expected principal bases. The exact basis may vary by jurisdiction, feature, relationship and the data actually processed. Special-Category Data also requires an Article 9 condition.

| Purpose                                                | Typical data                                  | Principal lawful basis                                            | Important qualification                                                        |
|--------------------------------------------------------|-----------------------------------------------|-------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Website access, essential sessions and requested pages | Device/network data, cookies, usage           | Contract or pre-contract steps; legitimate interests              | Deliver requested functionality, maintain sessions and ensure basic operation. |
| Account creation and administration                    | Account, contact, authentication, profile     | Contract; legitimate interests                                    | Create, authenticate, secure and manage the Account.                           |
| Adult eligibility and age gates                        | Age declaration, country, eligibility records | Contract; legitimate interests; legal obligation where applicable | Enforce adult-only access and processor/legal requirements.                    |

| Purpose                                                 | Typical data                                                                    | Principal lawful basis                                                            | Important qualification                                                   |
|---------------------------------------------------------|---------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| Enhanced age or identity verification                   | Verification result, identity data, provider reference; potentially facial data | Legal obligation or legitimate interests; consent/Explicit Consent where required | A point-of-collection notice must address biometric or facial processing. |
| Subscriptions, Wallet, Credits, PPV, chat and tips      | Transaction, wallet, entitlement, content-delivery data                         | Contract                                                                          | Provide paid services and maintain access records.                        |
| Payment authorization and reconciliation                | Payment metadata, processor references, billing status                          | Contract; legal obligation; legitimate interests                                  | Process charges, receipts, refunds and reconciliation.                    |
| Fraud, chargebacks and payment abuse                    | Risk signals, device links, transaction and support records                     | Legitimate interests; legal obligation; legal claims                              | Protect users, processors and CreamyPeach from fraud and losses.          |
| AI chat, media generation and requested personalization | AI Inputs, AI Outputs, conversation context, Chat Memory                        | Contract; legitimate interests; consent where optional                            | Deliver requested AI features and maintain service quality.               |
| Sensitive personalization                               | Adult-context preferences and Article 9 inferences                              | Explicit Consent, or another narrow Article 9 condition                           | Consent must be granular and withdrawable where relied upon.              |
| Content hosting, streaming and delivery                 | Uploads, media, metadata, entitlements                                          | Contract; legitimate interests                                                    | Provide content, protect rights and ensure delivery.                      |
| Moderation and platform safety                          | Messages, prompts, reports, classifications, evidence                           | Legitimate interests; legal obligation; vital interests; legal claims             | Detect minors, exploitation, threats, illegal content and policy abuse.   |
| Security and abuse prevention                           | Logs, IP, device, sessions, bot and malware signals                             | Legitimate interests; legal obligation where applicable                           | Protect confidentiality, integrity, availability and accounts.            |
| Customer support and complaints                         | Tickets, communications, transaction and account data                           | Contract; legitimate interests; legal obligation                                  | Resolve issues and meet complaint or rights duties.                       |
| Hosted Client onboarding and KYC                        | Identity, business, beneficial owner, tax, sanctions, payout data               | Pre-contract steps; contract; legal obligation; legitimate interests              | Assess eligibility, prevent fraud and satisfy processor/tax requirements. |
| Business Dashboard and Model Account                    | Authorized User, access logs, analytics, project and model data                 | Contract; legitimate interests                                                    | Provide role-based business services and security.                        |
| Character, ComfyUI, LoRA and chatbot services           | Client Materials, reference media, prompts, workflows, project records          | Contract; legitimate interests; Article 28 processing where applicable            | Perform SOW, protect rights and manage delivery.                          |
| Revenue share, commission and payouts                   | Revenue, deductions, statements, bank and tax data                              | Contract; legal obligation; legitimate interests                                  | Calculate 30/70 share, pay clients and maintain records.                  |
| Tax, accounting and platform reporting                  | Invoices, identity, tax, transaction and payout data                            | Legal obligation                                                                  | Comply with accounting, VAT, tax and applicable reporting regimes.        |
| Service analytics and improvement                       | Usage, performance, aggregated or pseudonymised data                            | Legitimate interests; consent for non-essential tracking                          | Understand performance and improve features with safeguards.              |
| Direct marketing and promotions                         | Contact, preferences, engagement, suppression records                           | Consent where required; legitimate interests where permitted                      | Honor opt-out and ePrivacy rules.                                         |
| Legal claims, rights and regulatory response            | Relevant account, content, payment, communication and evidence data             | Legal obligation; legitimate interests; Article 9(2)(f)                           | Establish, exercise or defend claims and answer lawful requests.          |

**26.2** Before launch, this matrix must be reconciled against the actual data-flow map, vendor contracts, cookie inventory, age-verification method, AI architecture, marketing configuration and Hosted Client access permissions.

## 27. Consent and Explicit Consent

**27.1** Where CreamyPeach relies on consent, the request will be separated from unrelated terms, written in clear language and presented through a genuine affirmative choice. Silence, inactivity or pre-ticked boxes will not be treated as valid consent.

**27.2** Consent will be specific to the stated purpose. Separate choices should be used for materially different purposes, such as non-essential cookies, email marketing, optional conversation memory and sensitive personalization.

**27.3** Where Article 9 requires Explicit Consent, CreamyPeach will use an express statement or equivalent unambiguous mechanism that specifically identifies the Special-Category Data and purpose.

**27.4** Consent may be withdrawn at any time through the relevant settings or privacy contact. Withdrawal does not affect processing that was lawful before withdrawal.

**27.5** If a feature cannot operate without the processing covered by withdrawn consent, CreamyPeach may disable that feature but should not restrict unrelated services merely because consent was refused or withdrawn.

**27.6** CreamyPeach will retain appropriate consent records, including the notice version, wording, timestamp, account or device identifier and withdrawal event.

**27.7** Consent is not accepted from minors because the Platform is adult-only.

## 28. Legitimate Interests

**28.1** CreamyPeach may rely on legitimate interests for account and service security, fraud and chargeback prevention, moderation, child-safety controls, rights protection, troubleshooting, service analytics, business administration, direct marketing where legally permitted and legal claims.

**28.2** Before relying on Article 6(1)(f), CreamyPeach should identify a specific lawful interest, assess whether the processing is necessary and balance that interest against the Data Subject's rights, expectations, vulnerability and the nature of the data.

**28.3** Heightened caution is required for private messages, adult-context data, Special-Category Data, extensive profiling, vulnerable persons, unexpected disclosure to Hosted Clients, behavioural advertising and processing that could produce serious consequences.

**28.4** Safeguards may include data minimisation, pseudonymisation, aggregation, short retention, role-based access, human review, exclusion of sensitive fields, opt-out, objection mechanisms and limiting use to security or safety purposes.

**28.5** Data Subjects have the right to object to processing based on legitimate interests.

**28.6** Legitimate interests will not be used where the processing is overridden by the individual's rights or where consent or another legal basis is specifically required.

## 29. Contract, Legal Obligation, Vital Interests and Legal Claims

**29.1** Contractual necessity applies only where processing is objectively necessary to perform the specific contract or take requested pre-contract steps. It does not justify optional advertising, unrelated model training or unnecessary sensitive profiling.

**29.2** For End Users, contractual purposes include account access, purchased subscriptions, Credits, content unlocks, paid chat, digital delivery, support and other requested services. For Hosted Clients, they include onboarding, hosting, dashboards, projects, revenue share, statements and payouts.

**29.3** Legal-obligation processing may include accounting, tax, VAT, court orders, regulator requests, sanctions, payment compliance, consumer records, data-protection duties, platform reporting and legally required safety actions. The exact obligation depends on the applicable law.

**29.4** Vital interests will be used only for genuine emergencies where processing is necessary to protect life or physical safety and another lawful basis is not reasonably available.

**29.5** Legal-claims processing may include preserving and using account, payment, content, communication, verification, safety and support records to establish, exercise or defend claims, respond to chargebacks, protect rights or cooperate with legal proceedings.

**29.6** When Special-Category Data is processed for legal claims, CreamyPeach may rely on Article 9(2)(f), subject to access restrictions and necessity.



## 30. Data Minimisation, Accuracy, Purpose Limitation and Privacy by Design

**30.1** CreamyPeach will seek to collect only data reasonably necessary for the relevant feature, role and risk. Optional profile fields should be clearly identified as optional.

**30.2** Age-verification and payment providers should be configured, where feasible, to return a verification or payment result rather than unnecessary raw identity or card data.

**30.3** Business Dashboards and Model Accounts should use role-based permissions and expose only the End-User Data, generated outputs, analytics and financial information required for the Authorized User's legitimate task.

**30.4** AI prompts, Chat Memory, preference profiles and training datasets should be separated from direct identifiers where feasible, and access should be logged and limited.

**30.5** CreamyPeach may ask individuals and Hosted Clients to update inaccurate information and may verify material business, tax, payment, rights or safety data before relying on it.

**30.6** Personal Data collected for one purpose will not be reused for a materially incompatible purpose without a compatibility assessment, a new lawful basis and any required notice or consent.

**30.7** New high-risk features, including biometric age verification, large-scale adult-interest profiling, sensitive AI memory, extensive Hosted Client access or new uses of real-person training data, should undergo a Data Protection Impact Assessment before deployment where required.

**30.8** Privacy-by-design review should be integrated into product planning, vendor selection, AI workflow design, access control, logging, data export, deletion and incident response.

## 31. Minors and Data We Do Not Intentionally Seek

**31.1** CreamyPeach is intended only for adults who have reached the applicable Age of Majority. CreamyPeach does not knowingly offer accounts or adult content to minors.

**31.2** If CreamyPeach reasonably believes that a minor has submitted Personal Data or accessed the Platform, it may restrict access, verify age, preserve necessary safety evidence, delete data where appropriate and make legally required reports.

**31.3** CreamyPeach does not intentionally request government identifiers, precise geolocation, health records, financial account passwords, real-world sexual-service information or third-party private data from ordinary End Users.

**31.4** Users should not submit another person's Personal Data, images, voice, likeness, private communications or identity documents unless they have authority and the submission is necessary for a supported purpose.

**31.5** Hosted Clients must not include minors, simulated minors, unlawful real-person data or unlicensed datasets in Character Assets, LoRA training inputs, chatbot instructions or other Client Materials.

**31.6** Deletion of suspected-minor data may be limited where temporary preservation is necessary to investigate, protect a child, comply with law or provide evidence to competent authorities.

## 32. Recipient and Disclosure Principles

**32.1** CreamyPeach discloses Personal Data only where the disclosure is reasonably connected to a stated purpose, permitted by the applicable lawful basis, proportionate to the sensitivity of the data and subject to appropriate safeguards.

**32.2** Recipient access is limited by role, purpose, Account, model, project, region and technical permission. A recipient is not entitled to access all information merely because it provides a service to CreamyPeach or participates in the Hosted Client Program.

**32.3** Before disclosing adult-context data, Special-Category Data, private messages, identity documents, biometric data or confidential Hosted Client materials, CreamyPeach should apply heightened necessity, access-control, contractual and transfer review.

**32.4** CreamyPeach may provide aggregated, de-identified, tokenized, pseudonymised or redacted information instead of directly identifying data where this is sufficient for the purpose.

**32.5** Recipients must not use Personal Data for their own unrelated purposes, combine it with unrelated data, train generalized AI models on it, sell it, disclose it onward or retain it longer than permitted unless they have an independent lawful basis and provide any required notice.

**32.6** Disclosures may be suspended, narrowed or terminated if a recipient fails due diligence, refuses required safeguards, experiences a security incident or uses data inconsistently with the governing contract.

## 33. Categories of Recipients

**33.1** Depending on the feature and relationship, Personal Data may be disclosed to cloud and infrastructure providers; payment and billing providers; fraud and security providers; age-assurance and identity providers; AI and automation providers; communications, support, analytics and attribution providers; Hosted Clients and their Authorized Users; professional advisers; insurers; auditors; regulators; courts and law-enforcement bodies.

**33.2** The categories above describe potential recipients. Not every recipient receives every data category, and not every category is used for every person.

**33.3** CreamyPeach should maintain an internal vendor and Subprocessor register identifying the legal entity, service, processing role, data categories, hosting and access locations, transfer mechanism, contract status and deletion settings.

**33.4** Where required by law or contract, CreamyPeach will make a current Subprocessor list or material-change notice available to the relevant Hosted Client or Data Subject.

**33.5** The identity of a specific Payment Processor, age-verification provider or Hosted Client may also be shown at checkout, onboarding, verification, dashboard access or another relevant point of collection.

## 34. Processors and Service Providers

**34.1** CreamyPeach may appoint Processors to perform services on its documented instructions, including hosting, storage, content delivery, support, email delivery, payment support, security, analytics, AI operations, age assurance, KYC, moderation tooling and data deletion.

**34.2** Processor contracts should address subject matter and duration, processing nature and purpose, data categories, Data Subjects, confidentiality, security, Subprocessors, assistance with rights and incidents, deletion or return, audit information and international transfers.

**34.3** Processors may process Personal Data only to provide the contracted service, meet documented legal obligations or protect the service as permitted by the DPA. They must not repurpose Personal Data for advertising, unrelated profiling or generalized AI training unless separately authorised and lawful.

**34.4** CreamyPeach may replace or add Processors as the Platform evolves, but must assess material privacy changes and provide any notice or objection opportunity required by the applicable Hosted Client contract or law.

**34.5** A provider that determines its own essential purposes may act as an independent controller for those activities. Its own privacy notice applies to that independent processing, but CreamyPeach remains responsible for selecting and disclosing the provider appropriately.

## 35. Payment, Banking, Billing and Fraud Providers

**35.1** Payment Processors, acquiring banks, card networks, billing agents, wallet providers and fraud vendors may receive transaction data, limited account and contact data, billing country, device and network signals, subscription details, transaction history, dispute evidence and fraud indicators.

**35.2** Full payment-card numbers and security codes are intended to be collected and stored by PCI-aligned Payment Processors rather than by CreamyPeach. CreamyPeach may receive payment tokens, card brand, last digits, expiry metadata, processor identifiers and payment status.

**35.3** Payment providers may act as Processors, independent controllers or both, depending on their compliance, anti-fraud, card-network, accounting and legal obligations. Their privacy notices may apply at checkout.

**35.4** CreamyPeach may disclose Terms acceptance, delivery, entitlement, login, device, communication, cancellation and support records to respond to chargebacks, unauthorized-use claims and payment disputes, subject to data minimisation.

**35.5** Hosted Client payout providers may receive business identity, beneficial-owner, bank, tax, revenue, commission, reserve, refund and risk information necessary to verify and execute payouts.

**35.6** Payment and payout access may be restricted where the provider, card network, bank or applicable law requires additional verification or prohibits a transaction, jurisdiction, content category or recipient.

## 36. Hosting, CDN, Storage and Infrastructure Providers

**36.1** CreamyPeach may use data-centre, cloud-compute, database, content-delivery, DNS, web-application firewall, object-storage, backup, logging, monitoring and email infrastructure providers.

**36.2** Infrastructure providers may process account identifiers, IP addresses, device and request data, encrypted credentials, content files, generated media, logs, database records, backups and support metadata according to their technical role.

**36.3** Private media should be protected through account entitlements, signed or time-limited access URLs, authorization checks and storage permissions rather than publicly accessible permanent links.

**36.4** CreamyPeach should select primary hosting regions deliberately and document any replication, backup, disaster-recovery or support access outside the primary region.

**36.5** Infrastructure contracts and configurations should restrict provider use, require appropriate security, define deletion and backup handling, and support the transfer mechanism applicable to each access location.

## **37. AI, Model, Automation and Content-Generation Providers**

**37.1** CreamyPeach may use third-party or self-hosted language, image, video, audio, moderation, recommendation, embedding, transcription, translation and automation systems to provide AI-assisted features.

**37.2** AI providers may receive prompts, conversation context, character instructions, generated outputs, safety labels, user preferences, project files or technical metadata only to the extent required for the configured feature.

**37.3** Where commercially and technically available, CreamyPeach should use enterprise or API settings that prohibit provider training on customer inputs and outputs, limit provider retention, restrict human review and support regional processing.

**37.4** No provider should receive raw identity documents, full payment details or unrelated Hosted Client confidential information merely because an AI feature is used. Sensitive fields should be removed, tokenized, redacted or segregated where feasible.

**37.5** CreamyPeach should assess the AI provider's data-use terms, security, model-training practices, Subprocessors, transfer locations, deletion options, incident history and ability to support rights before production use.

**37.6** AI provider terms do not replace CreamyPeach's obligations as controller or Processor. The live configuration and contract must match the statements made in this Privacy Policy.

## **38. Age Assurance, Identity, KYC and Verification Providers**

**38.1** Age-assurance, identity, liveness, document-verification, sanctions, business-verification and payout-KYC providers may process identifying, document, facial, device, contact, business and risk information for the specific verification requested.

**38.2** Where feasible, CreamyPeach should receive only a verification result, age threshold confirmation, risk outcome or limited extracted fields rather than a full identity document or biometric template.

**38.3** If facial images, liveness data or biometric templates are used, the collection interface must explain the provider, purpose, legal basis, retention and whether CreamyPeach or only the provider receives the raw data. Explicit Consent or another Article 9 condition may be required.

**38.4** Hosted Client KYC may include directors, beneficial owners, Authorized Users, tax status, bank ownership, sanctions screening and source-of-rights verification for character or training materials.

**38.5** Verification providers may act as Processors or independent controllers for regulatory, fraud and identity obligations. Their status and retention must be reflected in the contract and point-of-collection notice.

**38.6** Failure or refusal to complete required verification may result in denial of adult access, restricted features, delayed payouts, suspension or termination, subject to applicable rights and review.

## **39. Analytics, Support, Communications and Marketing Providers**

**39.1** CreamyPeach may use support-ticket, customer-relationship, email, transactional messaging, analytics, error-reporting, attribution, consent-management and communications providers.

**39.2** Support providers may process account, contact, transaction, device, communication, complaint and attachment data needed to resolve the request. Highly sensitive files should be restricted to trained personnel and removed when no longer necessary.

**39.3** Analytics providers may process pseudonymous identifiers, page or feature events, device data, referral information, performance data and conversion events. Private message content and adult-interest profiles should not be supplied to general advertising analytics.

**39.4** Marketing providers may receive contact details and campaign events only where the communication is lawful. Suppression records may be retained to respect opt-outs.

**39.5** Social-media platforms may receive attribution or event data if pixels, SDKs, conversion APIs or links are deployed. Such tools require a separate assessment, clear notice and consent or opt-out where required.

**39.6** CreamyPeach should avoid sending URL paths, page titles, profile names or event parameters that reveal explicit adult interests to third-party advertising platforms.

## **40. Professional Advisers, Corporate Transactions and Legal Recipients**

**40.1** CreamyPeach may disclose Personal Data to lawyers, accountants, auditors, tax advisers, cybersecurity specialists, insurers, banks, investors and other professional advisers where necessary for advice, assurance, financing, insurance, compliance or legal claims.

**40.2** Advisers are expected to be bound by professional secrecy, confidentiality, contract or law and to receive only information relevant to the engagement.

**40.3** In connection with a merger, investment, financing, restructuring, asset sale, insolvency or acquisition, relevant information may be disclosed under confidentiality and due-diligence safeguards.

**40.4** A successor must process Personal Data consistently with this notice unless it provides a new notice and establishes a lawful basis for a material change.

**40.5** Data rooms and transaction reviews should exclude or mask private chats, explicit media, raw identity records and sensitive user-level data unless genuinely necessary and subject to heightened controls.

## **41. Law Enforcement, Regulators, Safety and Rights Protection**

**41.1** CreamyPeach may disclose Personal Data where required by a valid law, court order, regulatory demand, tax obligation, payment rule or legally binding request.

**41.2** CreamyPeach may also disclose information where permitted and necessary to protect life or physical safety, investigate child exploitation, trafficking, non-consensual intimate content, fraud, cyberattack, account takeover, extortion, threats or serious illegal activity.

**41.3** Requests should be reviewed for authority, scope, jurisdiction, necessity and proportionality. CreamyPeach may seek clarification, narrow an overbroad request or challenge it where lawful and appropriate.

**41.4** Where legally permitted and not harmful to an investigation or person, CreamyPeach may notify the affected individual before or after disclosure. Notice may be delayed or withheld where prohibited.

**41.5** CreamyPeach should document the request, legal basis, records disclosed, decision maker, date, recipient and any confidentiality restriction.

**41.6** Voluntary disclosure of adult-context or Special-Category Data requires heightened review and must not be based solely on an informal or unverifiable request.

## **42. User-Directed, Public and Interactive Disclosures**

**42.1** Personal Data may be disclosed when a User intentionally publishes profile information, sends a message, submits content, contacts a Hosted Client, shares a link, requests a custom service or otherwise directs an interaction.

**42.2** Public or shared profile fields may be visible to other Users, search engines or external services depending on the feature. CreamyPeach should clearly distinguish public, restricted and private fields in the interface.

**42.3** A User must not publish another person's identity, contact details, intimate information, images, voice or private messages without authority and a lawful basis.

**42.4** Private messages are not public, but may be processed by CreamyPeach and authorised service providers for delivery, safety, support, fraud prevention, moderation and AI functions described in this notice.

**42.5** Where a feature sends information to an external service at the User's request, the external service's privacy terms apply after receipt.

**42.6** CreamyPeach may remove, restrict or preserve content if publication creates a safety, privacy, rights, fraud or legal risk.

## **43. Hosted Client and Authorized User Access**

**43.1** Hosted Clients may receive role-based access to a Business Dashboard or Model Account showing their own model configuration, generated outputs, content schedule, performance analytics, transaction summaries, revenue, commission, payout status, support matters and other agreed operational information.

**43.2** Hosted Clients do not receive unrestricted access to all End-User Data or to other Hosted Clients' data. Access must be limited to the specific model, project, Account, function and data elements approved for that Hosted Client.

**43.3** Access to private chat content, detailed User profiles or identifiable transaction data must be separately justified, disclosed and documented. Where operational needs can be met with aggregated or pseudonymous information, that form should be used.

**43.4** Authorized Users must have individual credentials, appropriate permissions and confidentiality duties. Shared credentials, credential resale and access by undeclared personnel are prohibited.

**43.5** A Hosted Client located outside the EEA may not receive remote access to EU Personal Data until the applicable role allocation, DPA, transfer mechanism and security requirements are completed.

**43.6** CreamyPeach may log dashboard access, exports, searches, changes and downloads and may restrict or revoke access for security, privacy, payment, legal or contractual reasons.

## **44. Hosted Client Segregation, Confidentiality and Permitted Use**

**44.1** Hosted Client data, model assets, project files, analytics and End-User Data should be logically segregated from data belonging to other Hosted Clients, with permission checks enforced at application and storage levels.

**44.2** Hosted Clients may use Personal Data received through the Platform only for the documented Hosted Client services, support, model operation, revenue reconciliation, lawful compliance and other purposes stated in the applicable agreement.

**44.3** Hosted Clients must not export End-User Data for unrelated marketing, sell or rent it, enrich external profiles, contact Users outside authorised channels, train unrelated AI models, create competing datasets or disclose it to unauthorised third parties.

**44.4** A Hosted Client that determines an independent purpose for Personal Data may become an independent controller and must provide its own lawful notice, legal basis, rights process, security and transfer safeguards. CreamyPeach may prohibit that independent use.

**44.5** Hosted Clients must promptly report suspected unauthorised access, credential compromise, accidental export, unlawful request, privacy complaint or security incident involving Platform data.

**44.6** At termination, Hosted Client access must be disabled promptly and exports, copies, API keys and local files must be returned, deleted or retained only where the contract and law permit.

## **45. Data Processing Agreements and Role Allocation**

**45.1** The Hosted Client Order Form, DPA or other contract must state whether CreamyPeach and the Hosted Client act as controller, joint controllers, controller and Processor, or independent controllers for each material processing activity.

**45.2** Where CreamyPeach processes Personal Data solely on a Hosted Client's documented instructions, the parties must enter into an Article 28-compliant DPA before processing, including security, Subprocessor, rights, incident, deletion and transfer provisions.

**45.3** Where the parties jointly determine purposes and essential means, an Article 26 arrangement must transparently allocate responsibilities for notices, lawful bases, rights, security, incidents, regulators and contact points.

**45.4** Revenue sharing, dashboard access or branding alone does not determine the legal role. The actual decisions concerning purposes, data fields, access, retention, communications and use control the analysis.

**45.5** CreamyPeach remains controller for its own billing, tax, fraud, safety, security, legal claims, platform integrity, processor management and business administration, even if it acts as Processor for another activity.

**45.6** No Hosted Client may instruct CreamyPeach to process Personal Data unlawfully. CreamyPeach may reject, suspend or terminate an instruction that violates law, rights, safety, payment rules or the Platform policies.

## **46. Subprocessor Governance and Vendor Due Diligence**

**46.1** Before appointing a material vendor or Subprocessor, CreamyPeach should assess legal identity, service scope, security, confidentiality, incident history, data locations, transfer mechanism, AI training terms, retention, deletion, access controls and audit information.

**46.2** Higher-risk review is required for vendors handling private chat, adult-context data, identity documents, biometric data, payment information, high-volume logs, Hosted Client datasets or production credentials.

**46.3** Subprocessors must be bound by data-protection obligations that are no less protective than the obligations applicable to the Processor for the relevant processing.

**46.4** CreamyPeach should maintain a change-management process for new regions, Subprocessors, AI models, data uses and material configuration changes and should update notices or contracts where required.

**46.5** A vendor's marketing claim, security certification or DPF listing does not replace contractual and technical verification. Certification scope and current status must be checked at the time of reliance.

**46.6** Vendor offboarding should include access revocation, credential rotation, data return or deletion confirmation, backup treatment and removal from the production data flow.

## **47. International Operations and Cross-Border Access**

**47.1** CreamyPeach is established in Romania, but Personal Data may be processed in other countries because Users, Hosted Clients, Authorized Users, vendors, support personnel, Payment Processors and AI providers operate internationally.

**47.2** A Cross-Border Transfer may occur through storage, replication, remote support, dashboard access, API transmission, email, payment processing, fraud review, content delivery, AI inference or legal disclosure.

**47.3** CreamyPeach will identify the applicable exporting jurisdiction and use a lawful transfer mechanism where required. A transfer mechanism does not eliminate the need for a lawful purpose, data minimisation, security and transparency.

**47.4** Hosted Clients must not assume that access from the United States, Canada, Israel or another non-EEA location is automatically permitted merely because the Hosted Client has a contract with CreamyPeach.

**47.5** CreamyPeach may restrict particular countries, vendors, support locations or Hosted Client access if an adequate transfer mechanism or sufficient supplementary measure cannot be established.

**47.6** Data may be subject to the laws of the country where it is processed, including lawful government-access powers. CreamyPeach addresses this risk through transfer assessments, contracts, encryption, minimisation and access controls where appropriate.

## **48. EU/EEA Adequacy Decisions and Recognised Destinations**

**48.1** Where the European Commission has adopted a valid adequacy decision covering the destination and recipient, Personal Data may be transferred from the EU/EEA without an additional Article 46 transfer safeguard, subject to the scope and conditions of that decision.

**48.2** As of 2 August 2026, the European Commission recognises Canada only for commercial organisations within the recognised scope, Israel, the United Kingdom, Switzerland and certain other jurisdictions as adequate, and recognises participating certified United States organisations under the EU-US Data Privacy Framework.

**48.3** Adequacy is recipient- and scope-sensitive. CreamyPeach must verify that the specific organisation, processing and data are covered and that the decision remains valid at the time of transfer.

**48.4** If an adequacy decision is suspended, narrowed, invalidated or no longer covers a recipient, CreamyPeach will seek another lawful mechanism, restrict access or stop the transfer.

**48.5** Adequacy does not authorise a recipient to use data for unrelated purposes or avoid controller, security, retention and rights obligations.

## **49. EU Standard Contractual Clauses, Transfer Assessments and Supplementary Measures**

**49.1** Where no applicable adequacy decision covers an EEA transfer, CreamyPeach may use the appropriate module of the EU SCCs, another approved Article 46 safeguard or a limited Article 49 derogation where its strict conditions are met.

**49.2** Before relying on the EU SCCs, CreamyPeach should map the transfer, identify the parties and roles, complete the annexes accurately, assess destination-law and government-access risk, and document whether supplementary measures are required.

**49.3** Supplementary measures may include encryption with keys controlled in the EEA, pseudonymisation, data-field reduction, split processing, access approvals, short retention, transparency commitments, challenge obligations, audit rights and restrictions on onward transfer.

**49.4** If effective protection cannot be achieved, the transfer must not proceed or must be suspended. Contract clauses alone are insufficient where they cannot be complied with in practice.

**49.5** Article 49 derogations are exceptional and should not be used as the routine mechanism for systematic Hosted Client access, ongoing cloud processing or regular AI-provider transfers.

**49.6** Transfer documentation should be reviewed after material legal changes, vendor changes, security incidents, new data categories or a change in government-access risk.



## 50. Transfers to the United States

**50.1** A transfer to a United States organisation may rely on the EU-US Data Privacy Framework only if the organisation is currently certified, the certification covers the relevant data and the organisation appears on the official DPF list at the time of transfer.

**50.2** A United States recipient that is not covered by the DPF requires another lawful mechanism, commonly the EU SCCs together with a Transfer Assessment and any necessary supplementary measures.

**50.3** United States Hosted Clients may access Platform data only through approved dashboards, APIs or support channels and only after the applicable transfer and role documentation is complete.

**50.4** Where U.S. state privacy laws apply, CreamyPeach may provide additional notices and rights concerning categories, sensitive data, sale, sharing, targeted advertising, profiling, retention and appeals.

**50.5** CreamyPeach should not disclose adult-context data, private chat or precise behavioural profiles to U.S. advertising networks for cross-context behavioural advertising.

**50.6** The Federal Trade Commission and state authorities may treat inaccurate privacy or AI-training promises as deceptive. CreamyPeach's contracts, technical settings and actual practices must therefore match this notice.

## 51. Transfers to Canada

**51.1** EU/EEA transfers to Canada may rely on the European Commission adequacy decision only for commercial organisations within its recognised scope. The applicability of that scope must be checked for each recipient.

**51.2** If a Canadian recipient is not covered by adequacy, CreamyPeach will use another valid transfer mechanism, such as the EU SCCs with a Transfer Assessment and appropriate safeguards.

**51.3** Canadian privacy law may require an organisation to remain accountable for Personal Data transferred to a service provider outside Canada and to use contractual or other means to provide comparable protection.

**51.4** Canadian Users and Hosted Client personnel should be informed that Personal Data may be processed in Romania, the EEA, the United States or other countries and may be accessible to authorities under the laws of those countries.

**51.5** Federal PIPEDA or substantially similar provincial laws may apply depending on the organisation, province, activity and data. A Canadian supplemental notice or contract should be used where local requirements differ.

**51.6** Canadian Hosted Clients remain responsible for ensuring that Client Materials and End-User Data they disclose to CreamyPeach were collected and transferred lawfully.

## 52. Transfers to Israel

**52.1** The European Commission recognises Israel as providing an adequate level of protection for transfers within the scope of the adequacy decision, subject to its conditions and continued validity.

**52.2** Where an Israeli Hosted Client transfers Personal Data to CreamyPeach or permits access from outside Israel, Israeli privacy and database-transfer rules may also apply independently of the GDPR.

**52.3** The parties should document the permitted transfer basis, receiving country, recipient obligations, onward-transfer restrictions, security and deletion requirements in the Hosted Client agreement or DPA.

**52.4** Israeli Hosted Clients must not upload identity documents, real-person intimate material, biometric data or third-party datasets without authority, lawful purpose, required notice and applicable consent.

**52.5** CreamyPeach may limit access or require additional contractual measures where the Israeli transfer route, database obligations or recipient status is uncertain.

**52.6** The EU adequacy decision for Israel does not remove the need to comply with Israeli law for outbound transfers from Israel or with GDPR for processing subject to GDPR.

## 53. United Kingdom, Switzerland and Other Transfer Frameworks

**53.1** Transfers from the United Kingdom must comply with the UK GDPR transfer rules, including UK adequacy regulations, the International Data Transfer Agreement, the UK Addendum to the EU SCCs, binding corporate rules or a valid exception.

**53.2** Where an appropriate UK safeguard is used, a transfer risk assessment may be required to determine whether protection is not materially lower after transfer.

**53.3** Transfers subject to Swiss law may use recognised adequacy, the adapted EU SCCs or another lawful safeguard, together with any Swiss-specific modifications and assessments required at the time.

**53.4** For other jurisdictions, CreamyPeach may apply local contractual clauses, consent, localization, registration, representative, security, notice or transfer-assessment requirements where applicable.

**53.5** A global customer base does not make every local privacy statute applicable. Coverage depends on establishment, targeting, thresholds, Data Subject location, data type and activity.

**53.6** Where local requirements conflict or cannot be satisfied, CreamyPeach may restrict the service, data category, feature, Hosted Client access or country.

## **54. Onward Transfers and Government Access Requests**

**54.1** A recipient may transfer Personal Data onward only where the onward transfer is permitted by the original contract, lawful basis and transfer mechanism and provides a substantially equivalent level of protection.

**54.2** Processors and Hosted Clients must disclose relevant Subprocessors or onward recipients and may require CreamyPeach's prior authorization according to the DPA.

**54.3** Recipients should notify CreamyPeach of a government demand unless prohibited, review its legality, seek narrowing, challenge unlawful or disproportionate demands and disclose only the minimum required data.

**54.4** CreamyPeach may publish or provide aggregate transparency information about government requests where lawful and operationally appropriate.

**54.5** Backdoor access, undisclosed administrative access, unrestricted support accounts and uncontrolled local exports are prohibited.

**54.6** If a recipient can no longer comply with the transfer safeguard, it must inform CreamyPeach promptly, and CreamyPeach may suspend access or require deletion or return.

## **55. Data Location, Remote Support and Localization**

**55.1** CreamyPeach should maintain a current data-location map identifying primary databases, media storage, backups, logs, AI processing, support access and Hosted Client access locations.

**55.2** Remote access is treated as processing in the access location for transfer and security assessment purposes where applicable, even if data remains physically stored in the EEA.

**55.3** Production access by personnel or contractors should be limited to approved countries, managed devices, authenticated sessions and documented support purposes.

**55.4** Where a jurisdiction requires local storage, local copy, regulator access, data export approval or appointment of a representative, CreamyPeach will assess whether the requirement applies before serving that market.

**55.5** Data localization does not guarantee that all support, fraud, payment or AI processing occurs locally. Any material exceptions should be disclosed and protected.

**55.6** CreamyPeach may offer region-specific processing or disable a feature if a provider cannot meet the required location or transfer controls.

## **56. AI Inputs, Outputs, Memory, Embeddings and Vector Stores**

**56.1** AI features may process prompts, conversation history, character instructions, preference signals, safety rules, generated text or media, feedback, embeddings, retrieval indexes and Chat Memory.

**56.2** Chat Memory may store selected facts, preferences, boundaries, prior purchases, model interaction state and conversation summaries to provide continuity. Sensitive memory should be limited, transparent, editable or removable where feasible.

**56.3** Embeddings and vector records may still be Personal Data if they relate to an identifiable person or can be linked back to an Account. They must not be treated as anonymous merely because they are numerical.

**56.4** CreamyPeach should separate identity, payment, safety, conversation and model-context data and should avoid placing unnecessary direct identifiers into prompts sent to external AI providers.

**56.5** AI inputs and outputs may be reviewed by authorised personnel for safety, support, quality, fraud or troubleshooting, but access should be logged and limited to a defined need.

**56.6** Users should not submit another person's private, intimate, biometric, identity or confidential information in prompts unless they are authorised and the feature supports that purpose.

**56.7** AI outputs may contain inferences, errors or sensitive content. They are governed by the same access, retention, safety and rights controls applicable to other Personal Data.

## 57. AI Training, Fine-Tuning and Product Improvement

**57.1** CreamyPeach will distinguish between processing required to provide an individual interaction and processing used to train, fine-tune, benchmark, evaluate or improve a model or generalized product.

**57.2** Private messages, adult-context data, Special-Category Data, Hosted Client confidential materials and identifiable real-person source files should not be used to train a generalized model unless a documented lawful basis, purpose-compatibility analysis, required notice, contractual authority and any required Explicit Consent are in place.

**57.3** CreamyPeach may use aggregated or appropriately de-identified metrics, synthetic examples, safety labels, error categories and limited evaluation samples for service quality, security and model testing where the risk of re-identification is controlled.

**57.4** Fine-tuning for a specific Hosted Client may use that Hosted Client's authorised Client Materials under the applicable Order Form and DPA. The resulting model, LoRA, embedding or configuration must not be reused for another client unless rights and data-protection requirements permit it.

**57.5** External AI providers must not train on CreamyPeach inputs or outputs contrary to the selected enterprise settings, contract or this notice.

**57.6** A material change from no-training or client-specific training to generalized training requires prior privacy review, updated notice, a valid legal basis and any required consent or opt-out before the new use begins.

**57.7** Deletion requests involving trained models require a technical and legal assessment because complete removal from model weights may not always be technically straightforward.

## 58. Hosted Client AI Projects, LoRA and Character Assets

**58.1** Hosted Client projects may include source images, reference media, captions, prompts, datasets, model weights, LoRAs, checkpoints, workflows, personality instructions, chatbot memory schemas, test conversations and generated deliverables.

**58.2** A Hosted Client must have lawful rights and authority for every real-person image, voice, dataset, likeness, trademark and confidential file it supplies and must identify any restrictions on use, geography, duration, model training or adult content.

**58.3** CreamyPeach may process project files to scope, create, test, host, maintain, secure, troubleshoot and deliver the commissioned character or chatbot service. Use for unrelated models or clients requires separate authorization.

**58.4** Where project files contain Personal Data or Special-Category Data, the Hosted Client agreement must allocate controller/Processor roles, lawful basis, Data Subject notice, rights handling, security, transfer and deletion.

**58.5** Project workspaces should be separated by Hosted Client and access limited to assigned personnel. Test outputs containing real-person likeness or sensitive data should not be used in public portfolios without permission.

**58.6** At project completion or termination, source files, intermediate artifacts, model weights and deliverables will be retained, returned or deleted according to the Order Form, intellectual-property terms, operational needs and applicable law.

## 59. Automated Moderation, Recommendations and Risk Scoring

**59.1** CreamyPeach may use automated rules, classifiers, similarity tools, content hashes, AI systems and risk models to rank content, recommend profiles, detect prohibited requests, moderate chat, identify fraud, protect Accounts and prioritize support.

**59.2** Signals may include content text or image features, Account age, payment and Chargeback history, device and IP risk, login patterns, transaction velocity, prior violations, report history, verification status and security events.

**59.3** Adult interests, sexual orientation or other Special-Category inferences must not be used for targeted advertising and should not be used for unrelated risk scoring. Any use for safety or content matching must be necessary, proportionate and supported by an Article 9 condition where required.

**59.4** Automated outputs may cause a prompt refusal, content label, reduced visibility, verification request, payment hold, security challenge, manual-review queue or temporary restriction.

**59.5** CreamyPeach should test material systems for false positives, bias, drift, security, explainability and disproportionate impact and should document significant changes.

**59.6** Automated signals are not treated as conclusive proof of wrongdoing. Material enforcement should consider context and human review where required or reasonably appropriate.

## 60. Solely Automated Decisions and Human Review

**60.1** CreamyPeach does not intend to make decisions based solely on automated processing that produce legal effects or similarly significant effects without a valid legal basis and the safeguards required by applicable law.

**60.2** A decision may be significant where it permanently terminates an Account, denies an earned payout, creates a serious fraud designation, blocks access based on identity or makes another substantial contractual determination.

**60.3** Where Article 22 GDPR applies, CreamyPeach will rely only on an available exception, provide meaningful information about the logic and expected consequences, and offer the right to obtain human intervention, express a view and contest the decision as required.

**60.4** Temporary security challenges, content recommendations, routine spam filtering and non-binding support prioritization do not necessarily constitute Article 22 decisions, but remain subject to fairness, transparency and accuracy obligations.

**60.5** Hosted Clients may not use Platform analytics or risk scores to make unrelated employment, credit, insurance, housing, immigration or other high-impact decisions about Users.

## 61. Cookies and Similar Technologies Overview

**61.1** CreamyPeach may use Cookies, local storage, session storage, pixels, tags, SDKs, server-side events, device identifiers and similar technologies to operate, secure, remember, measure and improve the Platform.

**61.2** The technologies used may collect or derive identifiers, session data, consent choices, device and browser information, IP address, referral data, page and feature events, performance data and conversion events.

**61.3** Where required by ePrivacy, GDPR or local law, non-essential technologies will not be activated until valid consent is obtained, and refusal must be as easy as acceptance.

**61.4** A detailed Cookie Policy or consent interface should identify current providers, purposes, categories, storage periods and third-party access. The live list must be generated from an actual scan and configuration review.

**61.5** Disabling certain technologies may affect preferences, login, media playback, fraud controls or feature availability, but refusing optional analytics or advertising technologies should not block core paid services unless lawful and strictly necessary.

**61.6** CreamyPeach should not place explicit model names, intimate preferences or sensitive chat information in URLs, pixel parameters or third-party analytics events.

## 62. Strictly Necessary and Functional Technologies

**62.1** Strictly necessary technologies may support login, session continuity, Account security, age-gate status, consent records, payment routing, load balancing, content entitlements, fraud prevention, language and essential Platform functions.

**62.2** These technologies may be used without consent where the applicable law permits because they are necessary to provide a service expressly requested or to secure the Platform.

**62.3** Functional technologies may remember optional preferences, display settings, selected model, media state, region, accessibility choices or chat configuration. Consent may be required depending on the technology and jurisdiction.

**62.4** Security and fraud technologies must remain proportionate. A “necessary” label must not be used to conceal advertising, unrelated analytics or optional tracking.

**62.5** Session technologies should expire when no longer needed, and persistent identifiers should have a defined lifetime linked to the purpose.

## 63. Analytics, Attribution, Advertising and Social Technologies

**63.1** CreamyPeach may use privacy-conscious analytics to understand feature use, errors, conversion, service performance, acquisition channels and aggregated customer journeys.

**63.2** Attribution technologies may connect an advertisement or referral to registration, subscription or purchase. Data fields should be minimized and should not disclose private chat, explicit content choices or Special-Category Data.

**63.3** Third-party advertising pixels, cross-site tracking and social-media SDKs present elevated privacy risks on an adult platform and should not be deployed until a DPIA or equivalent assessment, consent design, data-field review and vendor contract are complete.

**63.4** CreamyPeach does not intend to use adult-context or Special-Category Data to create advertising audiences or to target advertisements based on inferred sexual interests.

**63.5** Where a disclosure constitutes sale, sharing or targeted advertising under applicable U.S. or other law, CreamyPeach will provide the required notice and opt-out mechanism before or at the time of processing.

**63.6** Server-side conversion APIs are not automatically privacy-preserving; they remain disclosures and must be assessed and configured consistently with this notice.

## **64. Consent Management, Browser Signals and Electronic Marketing**

**64.1** CreamyPeach should use a consent-management platform or equivalent mechanism to record consent categories, timestamp, region, policy version, vendor choices and withdrawal.

**64.2** Consent must be freely given, specific, informed and unambiguous, and Explicit Consent must meet the higher standard required for Special-Category Data. Pre-ticked boxes and deceptive interfaces are not valid consent.

**64.3** Where applicable law requires recognition of a browser-based opt-out signal, including Global Privacy Control for covered sale or sharing activities, CreamyPeach will process the signal according to the applicable scope.

**64.4** Transactional messages concerning Accounts, security, purchases, subscriptions, payouts, legal notices and support may be sent where necessary for the service or legal obligation.

**64.5** Promotional email, SMS, push notifications or similar marketing will be sent only where permitted by the recipient's jurisdiction and choices. Each marketing channel should provide a practical opt-out.

**64.6** A record of an opt-out may be retained on a suppression list to prevent future marketing. Opting out of marketing does not stop essential service communications.

## **65. Security Governance and Confidentiality**

**65.1** CreamyPeach will maintain a risk-based security programme appropriate to the nature, volume, sensitivity and context of the Personal Data, including adult-context data, private communications, payment records, identity data and Hosted Client assets.

**65.2** Security responsibilities should be assigned to named personnel, supported by policies, asset and data inventories, access reviews, vendor governance, incident response, business continuity and regular management review.

**65.3** Personnel and contractors with access to Personal Data must be bound by confidentiality, receive role-appropriate training and access only what is required for their duties.

**65.4** CreamyPeach should apply privacy and security review before launching a material new feature, vendor, AI workflow, Hosted Client dashboard, data export or processing region.

**65.5** Security measures reduce risk but cannot guarantee absolute security. Users and Hosted Clients also have duties to secure their credentials, devices, email and local exports.

**65.6** Security documentation, penetration reports and architecture details may be confidential and disclosed only under appropriate controls.

## **66. Identity, Authentication, Access Control and Dashboard Security**

**66.1** Access to administrative, production, support and Hosted Client systems should use unique identities, least privilege, role-based access and multi-factor authentication where feasible and appropriate.

**66.2** Privileged access should be approved, time-limited where practicable, logged and periodically reviewed. Dormant, departed or compromised accounts must be disabled promptly.

**66.3** Hosted Client Authorized Users should receive access only to their assigned client, models, projects and functions. Cross-tenant access must be prevented through technical authorization checks and testing.

**66.4** Password resets, payout changes, data exports, new API keys and high-risk account changes may require step-up verification, confirmation or temporary delay.

**66.5** Shared administrator credentials, production credentials in chat, unsecured remote access and permanent vendor access are prohibited.

**66.6** CreamyPeach may monitor authentication, session, IP, device and administrative activity to detect account takeover, credential abuse and unauthorized access.

## **67. Encryption, Pseudonymization, Segregation and Key Management**

**67.1** Personal Data should be encrypted in transit using current secure protocols and encrypted at rest where appropriate to the system, risk and provider capabilities.

**67.2** Passwords must be stored using a strong one-way password-hashing method rather than reversible plaintext storage.

**67.3** Highly sensitive identifiers, identity files, biometric records, payment tokens, private media and secrets should be segregated, access-restricted or separately encrypted where feasible.

**67.4** Pseudonymous Account or project identifiers should be used in analytics, AI prompts, testing and support where direct identity is not necessary.

**67.5** Encryption keys, API secrets and signing keys should be protected through managed secrets storage, access separation, rotation and incident-response procedures.

**67.6** Encryption does not make data anonymous if CreamyPeach or another party can reconnect it to an individual.

## **68. Monitoring, Logging, Testing, Vulnerability and Supplier Security**

**68.1** CreamyPeach may log security events, administrative actions, login attempts, entitlement checks, payment events, data exports, API calls, moderation actions and system errors for security, audit, fraud and support purposes.

**68.2** Logs should exclude full payment-card data, raw passwords, unnecessary private-message content and sensitive tokens and should have restricted access and defined retention.

**68.3** CreamyPeach should use vulnerability scanning, dependency management, secure configuration, patching, code review, penetration testing and remediation processes proportionate to risk.

**68.4** A responsible vulnerability-reporting channel should allow good-faith reports without authorising destructive testing, data access or service disruption.

**68.5** Material suppliers should be assessed for security and incident response, and contracts should require prompt notice of incidents affecting CreamyPeach data.

**68.6** Test and development environments should use synthetic, anonymised or minimized data where feasible and should not receive uncontrolled copies of production adult-content or identity databases.

## **69. Security Incidents, Breach Assessment and Business Continuity**

**69.1** CreamyPeach will maintain procedures to detect, contain, investigate, remediate and document suspected Personal Data Breaches and security incidents.

**69.2** Incident assessment should consider the data categories, number of persons, identifiability, sensitivity, encryption, likely misuse, affected jurisdictions, Hosted Client roles and risk to rights and freedoms.

**69.3** Where CreamyPeach acts as Processor, it will notify the relevant controller without undue delay according to the DPA. Where CreamyPeach acts as controller, it will assess regulator and individual notification duties under applicable law.

**69.4** CreamyPeach may preserve logs, restrict Accounts, rotate credentials, suspend integrations, notify Payment Processors or Hosted Clients and involve security specialists, insurers or authorities as appropriate.

**69.5** Business-continuity and disaster-recovery measures may include backups, restoration testing, redundancy, recovery priorities and alternative service arrangements.

## **70. Retention Principles**

**70.1** CreamyPeach retains Personal Data only for as long as reasonably necessary for the purpose described, contractual performance, legal obligations, accounting and tax, payment disputes, safety, fraud prevention, security, rights, legal claims and documented business needs.

**70.2** Retention decisions consider data sensitivity, volume, identifiability, Account status, transaction and entitlement needs, limitation periods, processor rules, Hosted Client contracts, backup cycles and deletion feasibility.

**70.3** Different fields within the same record may have different retention periods. Direct identifiers may be removed while a limited transaction, fraud or statistical record is retained.

**70.4** Retention may be extended by a complaint, Chargeback, investigation, litigation hold, authority request, unresolved payout, safety incident or statutory requirement.

**70.5** Retention may be shortened where data is inaccurate, unlawfully collected, no longer needed, withdrawn from consent-based processing or subject to a valid deletion request.

**70.6** The periods below are proposed operational targets for the final policy and must be reconciled with actual deletion jobs, processor settings and Romanian, EU and other applicable law before publication.



## 71. Retention Schedule - Accounts, Chat, AI and Content

**71.1** Account and profile data: generally for the life of the Account and up to 24 months after closure, unless a shorter deletion request applies or a longer legal, fraud, safety or dispute need exists.

**71.2** Terms, privacy, age confirmation and consent records: generally for the relationship and up to 5 years after the relevant interaction or Account closure, or longer where required to demonstrate compliance or defend a claim.

**71.3** Private chat and prompts: generally while the Account and feature are active and for up to 12 months after deletion or closure, subject to user controls, paid-delivery records, safety flags, Hosted Client arrangements and legal holds.

**71.4** Chat Memory, embeddings and personalization profiles: generally until the feature is reset, consent is withdrawn, the Account is closed or 12 months after the last relevant interaction, unless a shorter user control or longer safety need applies.

**71.5** Generated media and content entitlements: generally while the content is offered and the Account has access, plus up to 24 months after Account closure or entitlement termination for restoration, disputes and rights management.

**71.6** Moderation copies and prohibited-content evidence: retained only as long as necessary for enforcement, repeat-offender controls, safety reporting, legal claims and authority cooperation, with access restricted.

**71.7** Product analytics events: generally up to 24 months in identifiable or pseudonymous form, after which they should be aggregated, de-identified or deleted unless a shorter consent setting applies.

## 72. Retention Schedule - Payments, KYC, Hosted Client and Support Data

**72.1** Invoices, accounting registers and supporting tax records: generally for 5 years calculated from 1 July of the year following the end of the financial year in which they were prepared, subject to statutory exceptions, later amendments and longer retention where another law, audit or legal hold requires.

**72.2** Payment, Wallet, entitlement, refund and Chargeback records: generally for the transaction relationship and up to 5 years after final resolution, subject to processor, card-network, tax and legal requirements.

**72.3** Fraud, security and account-takeover records: generally up to 5 years after the event or last linked activity where necessary to prevent repeated abuse, with periodic review and minimisation.

**72.4** Age-verification results: generally while adult access is active and up to 24 months after Account closure. Raw identity images, facial images or biometric templates should be retained by the verification provider only for the shortest configured period unless a dispute, fraud or legal obligation requires more.

**72.5** Hosted Client KYC, payout and tax records: generally for the business relationship and at least 5 years after termination or final payout where required for tax, payment, sanctions, fraud or legal claims.

**72.6** Hosted Client project files, LoRAs, workflows and character assets: according to the Order Form, generally during the project and hosting term plus up to 24 months for support, transition and dispute resolution unless return or earlier deletion is agreed.

**72.7** Support tickets and ordinary complaints: generally up to 3 years after closure. Serious safety, rights, payment or legal matters may be retained up to 5 years or longer where necessary.

**72.8** Marketing contact data: until opt-out, invalidity or Account closure, with a limited suppression record retained up to 5 years to ensure the opt-out is respected.

### Proposed Retention Matrix - Implementation Validation Required

| Data group                   | Proposed target                       | Main reason                              |
|------------------------------|---------------------------------------|------------------------------------------|
| Account/profile              | Active term + up to 24 months         | Service, restoration, disputes, security |
| Chat/prompts/memory          | Active feature + up to 12 months      | Delivery, continuity, safety, support    |
| Generated media/entitlements | Active access + up to 24 months       | Access, rights, restoration, disputes    |
| Payments/wallet/chargebacks  | Up to 5 years after final resolution  | Accounting, tax, disputes, fraud         |
| Hosted Client KYC/payout     | Relationship + at least 5 years       | Tax, payouts, fraud, sanctions, claims   |
| Project files/LoRA/workflows | Contract term + up to 24 months       | Hosting, support, handover, disputes     |
| Support/ordinary complaints  | Up to 3 years                         | Customer service and claims              |
| Safety/fraud/legal evidence  | Up to 5 years or legal-hold period    | Safety, repeat abuse, legal claims       |
| Backups                      | Rolling cycle, normally up to 90 days | Resilience and recovery                  |

## 73. Deletion, Anonymisation, Backups, Legal Holds and Derived Data

**73.1** At the end of the applicable retention period, Personal Data will be deleted, anonymised, overwritten, access-restricted or placed beyond ordinary use according to the system and legal requirement.

**73.2** Deletion from live systems may not immediately remove data from encrypted backups. Backups should follow a defined rolling cycle, normally targeted at no more than 90 days, and should not be restored except for recovery or legal need.

**73.3** If a backup is restored, deletion and restriction instructions should be reapplied where technically feasible.

**73.4** A Legal Hold may suspend ordinary deletion for specific records relevant to a dispute, investigation, authority request, Chargeback, safety matter or anticipated claim. The hold should be scoped, documented and reviewed.

**73.5** Derived data such as risk flags, embeddings, summaries or model-evaluation labels must be included in deletion and rights workflows where they remain Personal Data.

**73.6** Anonymisation requires that identification is no longer reasonably possible, taking account of available means. Pseudonymised data remains Personal Data.

**73.7** Processor and Hosted Client deletion obligations must include copies, exports and Subprocessors, subject to lawful retention and documented exceptions.

## **74. Aggregated, De-identified and Statistical Data**

**74.1** CreamyPeach may create aggregated, de-identified or statistical information for service measurement, capacity planning, safety, fraud trends, model performance, commercial reporting and Hosted Client analytics.

**74.2** De-identification should remove direct identifiers and reduce combinations, small groups, free text and rare events that could reasonably identify a person.

**74.3** Hosted Client dashboards should use aggregation thresholds and pseudonymous metrics where identifiable User-level data is not necessary.

**74.4** CreamyPeach and recipients must not attempt to re-identify properly anonymised or de-identified data except for authorised security testing or to assess the effectiveness of de-identification.

**74.5** If aggregated or de-identified information can still reasonably be linked to a person, it will be treated as Personal Data under this notice.

## **75 United States, Canada, Israel and Other Local Privacy Overlays**

**75.1** This global notice is intended to provide a common privacy framework. Additional mandatory disclosures may apply based on the individual's residence, the Hosted Client's establishment, local thresholds and the processing activity.

**75.2** For United States residents, a supplemental notice may describe categories collected and disclosed, sensitive Personal Data, retention, sale or sharing, targeted advertising, profiling, authorised agents and appeal rights under applicable state law.

**75.3** For Canadian residents, federal PIPEDA or substantially similar provincial laws may require meaningful consent, reasonable purposes, accountability, safeguards, access and breach handling, including transparency about processing outside Canada.

**75.4** For Israeli residents or Hosted Clients, the Privacy Protection Law, regulations concerning database security and transfers abroad, and related authority guidance may require additional contractual, database, security or notice measures.

**75.5** For UK and Swiss residents, UK GDPR or Swiss data-protection requirements may supplement this notice, including local transfer and representative rules.

**75.6** CreamyPeach may publish a jurisdiction-specific addendum rather than rewriting the entire policy.

**75.7** No clause limits a mandatory local right or protection that cannot lawfully be waived.

## **76. Sale, Sharing, Targeted Advertising and Sensitive Data**

**76.1** CreamyPeach does not sell Personal Data for monetary consideration as part of its ordinary business model and does not sell or share Personal Data of known minors.

**76.2** CreamyPeach does not use adult-context data, private chat, sexual-orientation inferences, identity documents, biometric data or other Special-Category Data for targeted advertising or cross-context behavioural advertising.

**76.3** Certain analytics, advertising, social-media or attribution disclosures may be treated as "sale," "sharing" or targeted advertising under some laws even where no money is exchanged. Such tools must be identified and assessed before deployment.

**76.4** Where a covered activity is used, CreamyPeach will provide the required notice, consent or opt-out mechanism and will honour applicable browser-based opt-out signals.

**76.5** CreamyPeach will not use a rights request or privacy choice to discriminate unlawfully, but feature differences reasonably related to the data and service may apply.

## **77. How to Submit a Privacy Rights Request**

77.1 A Data Subject may submit a Rights Request through an available Request Portal, an authenticated Account control or by emailing [privacy@creamypeach.com](mailto:privacy@creamypeach.com). The request should identify the right being exercised and provide enough information to locate the relevant records.

77.2 Requests should be sent from the email address connected to the Account where reasonably possible. A person without an Account may describe the relevant interaction, approximate date, email address, transaction reference, Hosted Client relationship or other locator.

77.3 A request need not use legal terminology. CreamyPeach will assess the substance of the communication and may ask a focused question where the requested action is unclear.

77.4 General support, billing disputes, content reports and account-access problems may be routed to the appropriate team, while any embedded privacy right will remain tracked as a Rights Request.

77.5 CreamyPeach will provide reasonable accessibility assistance and will not require a person to purchase a service or create a new paid Account solely to exercise a privacy right.

## **78. Identity, Account-Control and Authority Verification**

78.1 CreamyPeach must take reasonable steps to verify that a requester is the Data Subject or is authorized to act for that person before disclosing, exporting, correcting or deleting Personal Data.

78.2 Verification will be proportionate to the sensitivity of the data and the risk of harm. Private chat, adult-context preferences, identity records, payment history, Hosted Client KYC and security logs require stronger verification than an ordinary marketing opt-out.

78.3 Verification may use authenticated Account access, a confirmation link, known transaction or account information, a processor reference, a signed declaration, proof of authority or a narrowly tailored identity check. CreamyPeach will seek to avoid collecting unnecessary identity documents.

78.4 CreamyPeach will not ask a requester to disclose a password, full payment-card number, secret authentication code or more Age Verification Data than reasonably necessary.

78.5 If identity or authority cannot be reasonably verified, CreamyPeach may request additional information, narrow the response, use a secure in-account method or refuse the request and explain the applicable reason and complaint route.

78.6 Verification records will be used to prevent unauthorized disclosure and demonstrate compliance and will be retained only as reasonably necessary under the retention rules in stated before.

## **79. Authorized Agents, Representatives and Rights on Behalf of Others**

79.1 A Data Subject may use an authorized agent or legally recognized representative where applicable law permits.

79.2 CreamyPeach may require signed authority, a power of attorney, proof of guardianship or other legally sufficient evidence and may contact the Data Subject directly to confirm identity and authority unless the law provides otherwise.

79.3 An agent must not use false documents, impersonation, compromised credentials or information obtained through coercion. CreamyPeach may report suspected fraud or account takeover.

79.4 A Hosted Client or Authorized User cannot exercise an End User's personal rights merely because the person interacted with a Hosted Model. The Hosted Client must demonstrate a valid legal role or forward the request under the applicable DPA.

79.5 Where the Data Subject is deceased, incapacitated or otherwise unable to act, CreamyPeach will follow the rights and authority rules of the applicable jurisdiction and may preserve the Account while authority is assessed.

## **80. Response Times, Format, Fees and Communication**

80.1 For requests governed by the GDPR, CreamyPeach will provide information on action taken without undue delay and in principle within one month after receiving the request. That period may be extended by up to two additional months where necessary because of complexity or number of requests, with notice and reasons provided within the first month.

80.2 Different statutory deadlines may apply under Canadian, United States, Israeli, UK, Swiss or other law. CreamyPeach will apply the legally controlling deadline and may respond earlier.

80.3 Responses will ordinarily be provided electronically through a secure Account, encrypted link or the verified email channel used for the request. A commonly used electronic format will be used unless another lawful format is reasonably requested.

80.4 Rights Requests are ordinarily handled free of charge. Where permitted by law, CreamyPeach may charge a reasonable administrative fee or refuse to act on requests that are manifestly unfounded or excessive, particularly because of repetition, and bears the burden of demonstrating that conclusion.

80.5 If CreamyPeach does not act on a request, it will explain the reasons and available complaint or judicial-remedy routes within the period required by applicable law.

80.6 Time may pause only where and to the extent permitted by applicable law while CreamyPeach reasonably awaits information necessary to verify identity, authority or the scope of the request.

## **81. Right to Information and Transparency**

81.1 Individuals may receive clear information about the identity of the controller, data categories, sources, purposes, lawful bases, recipients, transfers, retention, rights and relevant automated processing, as described in this notice and layered notices.

81.2 CreamyPeach may provide contextual notices at age verification, checkout, chat, AI personalization, custom-content submission, Hosted Client onboarding or another collection point where the general notice would not provide sufficient detail.

81.3 Materially different processing will not be hidden behind vague language. Where a new purpose is incompatible with the original purpose, CreamyPeach will identify a valid legal basis and provide any notice or choice required before the new processing.

81.4 Individuals may ask [privacy@creamypeach.com](mailto:privacy@creamypeach.com) for clarification about a processing activity that is not reasonably explained by the published notices.

## **82. Right of Access and Copies**

82.1 Subject to applicable law, a Data Subject may request confirmation whether CreamyPeach processes Personal Data about that person and may obtain access to the Personal Data and required supplementary information.

82.2 An access response may include relevant Account and profile data, transaction and entitlement records, chat or prompt data retained by CreamyPeach, Chat Memory, support history, preferences, moderation information, recipients or recipient categories, retention information, data sources and relevant automated-decision information.

82.3 The first copy required by the GDPR will be supplied without charge. Additional copies may be subject to a reasonable administrative fee where legally permitted.

82.4 Access is a right to Personal Data and required information, not necessarily to every original document, complete internal file, proprietary workflow, source code, security rule, fraud model or model weight.

82.5 CreamyPeach may redact, summarize, separate or withhold information where disclosure would adversely affect the rights and freedoms of another person, reveal another user's private communication, compromise security or fraud controls, violate privilege or confidentiality, or fall within another lawful exception.

82.6 A refusal or limitation will not be broader than necessary. Where possible, CreamyPeach will provide the remainder of the response or a meaningful description that does not create the protected risk.

## **83. Right to Rectification and Completion**

83.1 A Data Subject may request correction of inaccurate Personal Data and completion of incomplete Personal Data, taking account of the purpose of the processing.

83.2 Some Account, profile, contact and preference information may be corrected directly through Account settings. Records that affect invoices, transactions, fraud, KYC, age verification or legal evidence may require supporting information and may be corrected through an annotation rather than destructive overwriting.

83.3 Opinions, predictions, risk assessments and AI-generated inferences are not automatically inaccurate because the person disagrees with them. CreamyPeach will, however, assess whether the underlying data are wrong, whether the inference is misleading for its purpose, and whether correction, annotation, restriction or deletion is appropriate.

83.4 Where required, CreamyPeach will communicate a rectification to recipients to whom the Personal Data were disclosed unless impossible or involving disproportionate effort and will inform the Data Subject about those recipients upon request.

## **84. Right to Erasure and Account Deletion**

84.1 A Data Subject may request erasure where Personal Data are no longer necessary, consent is withdrawn and no other legal ground applies, processing is unlawful, a valid objection prevails or erasure is otherwise required by law.

84.2 Closing an Account stops ordinary future use but does not necessarily erase every record immediately. An Account-deletion request will be treated as an erasure request for associated Personal Data and assessed against the exceptions in Clause 89.

84.3 CreamyPeach will seek to delete or irreversibly anonymize eligible Account, profile, preference, Chat Memory, prompt, content and analytics data from active systems and instruct relevant Processors as required.

84.4 Deletion may also revoke content entitlements, disable access to purchased or generated content, close subscriptions and remove personalization. The person should download any portable information they wish to retain before deletion where the service provides that option.

84.5 Deletion from active systems may not immediately remove encrypted backup copies. Backup handling, restoration controls and deletion reapplication are described in Clause 75.

84.6 CreamyPeach will not intentionally use data retained solely under a deletion exception for ordinary marketing or unrelated personalization.

## **85. Erasure Exceptions, Legal Retention and Suppression Records**

85.1 The right to erasure is not absolute. CreamyPeach may retain limited Personal Data where necessary for legal obligations, accounting or tax records, freedom of expression and information where applicable, public-interest duties, establishment or defence of legal claims, fraud prevention, security, chargebacks, safety, sanctions, rights protection or another lawful exception.

85.2 Transaction, invoice, Wallet, entitlement, refund and Chargeback records may be retained in minimized form even after Account deletion where required for accounting, processor reconciliation, dispute evidence or legal compliance.

85.3 CreamyPeach may retain a limited suppression record to respect an opt-out, block a prohibited person or payment instrument, prevent repeated fraud, preserve a content hash, record that consent was withdrawn or demonstrate that a request was completed.

85.4 A Legal Hold may suspend deletion for specifically relevant data. The hold will be documented, access-restricted and reviewed, and unrelated data will remain subject to ordinary deletion.

85.5 Where complete deletion is not technically or legally possible, CreamyPeach may restrict the data from ordinary use and explain the retained category and reason to the extent disclosure does not compromise security, privilege or legal obligations.

## **86. Right to Restriction of Processing**

86.1 A Data Subject may request restriction where accuracy is contested while verification occurs, processing is unlawful but erasure is opposed, CreamyPeach no longer needs the data but the person needs it for legal claims, or an objection is being assessed.

86.2 Restricted data may be marked, isolated, access-limited or removed from ordinary workflows. It may still be stored and, where legally permitted, used with consent, for legal claims, to protect another person or for important public-interest reasons.

86.3 Restriction may affect service functionality, including personalization, AI memory, content generation, payment access, fraud review or Hosted Client dashboard features, where the restricted data are necessary for the feature.

86.4 CreamyPeach will inform the Data Subject before lifting a restriction where required and will notify relevant recipients as required by applicable law.

## **87. Right to Data Portability**

87.1 Where processing is based on consent or contract and carried out by automated means, a Data Subject may request Personal Data that the person provided in a structured, commonly used and machine-readable format.

87.2 Portable data may include eligible Account details, user-supplied profile data, prompts, messages, preferences and transaction information, but does not automatically include inferred data, proprietary scoring, CreamyPeach-created analytics, rights of others, security secrets or third-party copyrighted material.

87.3 Where technically feasible and legally required, CreamyPeach may transmit eligible data directly to another controller at the Data Subject's request. CreamyPeach does not guarantee interoperability with another service.

87.4 Portability does not erase the data, cancel the Account or override retention obligations. A separate erasure or closure request may be required.

## **88. Right to Object and Direct-Marketing Objections**

88.1 A Data Subject may object, on grounds relating to the person's particular situation, to processing based on legitimate interests or a public-interest ground, including related Profiling.

88.2 CreamyPeach will stop the objected processing unless it demonstrates compelling legitimate grounds overriding the person's interests, rights and freedoms or the processing is needed for legal claims.

88.3 A person may object at any time to direct marketing, including Profiling related to direct marketing. CreamyPeach will stop that marketing without requiring the person to show particular grounds.

88.4 Marketing opt-out does not stop essential service, security, billing, legal or transactional communications. A limited suppression record may be retained to honor the choice.

88.5 Where legally required, CreamyPeach will honor recognized browser-based opt-out preference signals for covered sale, sharing or targeted-advertising activities.

## **89. Withdrawal of Consent and Explicit Consent**

89.1 Where processing relies on Consent or Explicit Consent, the Data Subject may withdraw it at any time through the relevant setting, consent interface or by contacting [privacy@creamyteach.com](mailto:privacy@creamyteach.com).

89.2 Withdrawal will be as easy as giving consent where required and will not affect the lawfulness of processing performed before withdrawal.

89.3 After withdrawal, CreamyTeach will stop the consent-based processing unless another lawful basis independently applies and has been properly disclosed. CreamyTeach will not silently replace withdrawn consent with legitimate interests for the same sensitive optional purpose.

89.4 Withdrawing optional sensitive personalization may reset Chat Memory, recommendation profiles, preference inferences or related embeddings and may reduce personalization without necessarily closing the Account.

89.5 Consent records and a limited withdrawal record may be retained to demonstrate compliance and prevent the processing from being reactivated unintentionally.

## **90. Adult-Context, Special-Category and Sensitive-Data Controls**

90.1 Because CreamyTeach is an adult-only service, interactions, purchases, content interests or chat may reveal or support inferences concerning sex life or sexual orientation and therefore require heightened confidentiality.

90.2 Where CreamyTeach relies on Explicit Consent for optional sensitive personalization, the person may view, reset or withdraw that choice through the available feature or privacy request channel.

90.3 CreamyTeach will not use Adult-Context Data, private chat, sexual-orientation inferences, identity documents or Biometric Data for targeted advertising or cross-context behavioural advertising.

90.4 A request to limit sensitive-data use under applicable United States law will be honored where the law applies. The service may continue narrowly permitted uses such as security, service delivery, verification, legal compliance and protection against fraud.

90.5 CreamyTeach will use secure delivery and heightened verification for copies containing Adult-Context Data and may separate such information from a general export.

## **91. Automated Decisions, Profiling and Human Review**

91.1 CreamyTeach may use automated tools for recommendations, content classification, personalization, moderation triage, fraud and security scoring, entitlement checks, payment routing and service operations

91.2 CreamyTeach does not intend to make a decision based solely on automated processing that produces legal or similarly significant effects unless the decision is necessary for a contract, authorized by law or based on Explicit Consent, and all required safeguards are provided.

91.3 Where Article 22 GDPR or a comparable law applies, the person may request human intervention, express a point of view and contest the decision. The reviewer will have authority to reassess relevant information rather than merely repeat the automated outcome.

91.4 Temporary automated security measures may be used to contain suspected fraud, account takeover, prohibited content or payment risk while a matter is reviewed. A user may use the appeal or support route identified in the notice or decision message.

91.5 CreamyTeach may protect confidential fraud methods, security rules and third-party rights while still providing meaningful information about the principal factors, consequences and available safeguards where required.

## **92. AI Inputs, Outputs, Chat Memory, Embeddings and Derived Data Rights**

92.1 Rights workflows will include AI Inputs, AI Outputs, Chat Memory, embeddings, summaries, preference profiles, safety classifications and other derived records where they remain Personal Data and CreamyTeach controls them.

92.2 A person may request correction, reset, deletion, restriction or access for eligible Chat Memory and personalization records. CreamyTeach may regenerate or remove a summary rather than alter an immutable historical message where that approach better preserves record integrity.

92.3 An embedding or model-related artefact will not be treated as anonymous merely because it is not human-readable. CreamyTeach will assess whether it can reasonably be linked to an individual and will apply rights where legally and technically applicable.

92.4 A request concerning training data or a client-specific LoRA will be assessed against the data's identifiability, the controller role, contractual rights, technical feasibility, rights of others and any lawful retention need.

92.5 CreamyTeach will not claim that deletion of a prompt necessarily reverses every statistical effect on a model. Where direct removal from a trained model is not reasonably possible, CreamyTeach will apply available safeguards, stop future use where required and explain the practical outcome.

92.6 Generalized AI training using identifiable private chat or Adult-Context Data requires the separate assessments and controls described in Clause 59 and is not authorized merely by acceptance of this Privacy Policy.

## **93. Rights Concerning Hosted Clients, Model Accounts and Dashboards**



93.1 A Rights Request may involve data controlled by CreamyPeach, a Hosted Client or both. CreamyPeach will identify and route the request according to the documented role allocation without requiring the person to understand that allocation in advance.

93.2 Where CreamyPeach is the controller, it remains responsible for responding even if relevant data are stored by a Processor or displayed in a Hosted Client dashboard.

93.3 Where a Hosted Client is an independent controller, CreamyPeach may provide the client's contact details, forward the request with the person's knowledge, preserve relevant evidence and assist as required by contract or law.

93.4 Hosted Clients and Authorized Users must promptly forward Rights Requests relating to CreamyPeach-controlled End-User Data and must not independently export, delete, alter or disclose Platform data outside their authorized role.

93.5 Dashboard exports, local copies and data placed in a Hosted Client's independent systems remain subject to that Hosted Client's own legal obligations. CreamyPeach will use contractual controls and reasonable assistance but cannot represent that it controls an independent recipient's systems.

93.6 Termination of a Hosted Client relationship does not extinguish End-User rights. Transition, return, deletion and retention obligations must follow the applicable Order Form, DPA and this notice.

#### **94. Processor, Subprocessor and Recipient Cooperation**

94.1 CreamyPeach will communicate valid rectification, erasure or restriction instructions to relevant Processors and recipients where required, unless this proves impossible or involves disproportionate effort.

94.2 Processor contracts should require reasonable assistance with Rights Requests, secure return or deletion, breach information and evidence of compliance.

94.3 CreamyPeach may not be able to delete data held by an independent controller for its own legal purposes, such as a payment processor, bank, card network, tax authority, regulator or law-enforcement body. The independent controller's notice and rights process applies to its processing.

94.4 Upon request, CreamyPeach will provide information about recipients to the extent required by law and consistent with the rights of others, security and confidentiality.

94.5 A request does not require CreamyPeach to recall content or data that another person lawfully obtained and independently controls unless applicable law imposes that obligation.

#### **95. Content, Media, Depicted Persons and Privacy Complaints**

95.1 A person who believes content depicts, identifies, impersonates or exposes that person without lawful authority may submit a privacy, non-consensual-intimate-content, impersonation or rights complaint through the designated reporting channel.

95.2 The report should identify the content location, the complainant's connection to the content, the requested action and available supporting information. CreamyPeach may use proportionate identity or liveness verification to prevent fraudulent takedowns.

95.3 CreamyPeach may temporarily restrict access while assessing consent, identity, age, rights and safety. Copyright complaints may be handled separately under the Copyright Policy.

95.4 Removal from public or user access does not necessarily require immediate destruction of a restricted evidentiary copy needed for safety, legal claims, authority reporting, repeat-offender prevention or proof of action taken.

95.5 False, malicious or impersonating complaints are prohibited, but a good-faith report will not be penalized merely because evidence is incomplete or the legal conclusion differs.

#### **96. United States State Privacy Rights**

96.1 If a United States state privacy law applies to CreamyPeach and the requester, the person may have rights to know or access, correct, delete and obtain a portable copy of covered Personal Data, subject to statutory exceptions.

96.2 Depending on the state and CreamyPeach's activities, a person may also have rights to opt out of sale, sharing, targeted advertising or qualifying Profiling and to limit certain uses or disclosures of Sensitive Personal Data.

96.3 CreamyPeach does not sell Personal Data for monetary consideration as part of its ordinary business model and does not use Adult-Context Data, private chat or Special-Category Data for targeted advertising. Clause 78 explains that some non-monetary advertising disclosures can nevertheless be regulated as sale or sharing.

96.4 Where required, CreamyPeach will honor an authorized agent and a recognized opt-out preference signal, provide an appeal route for a denied request and avoid unlawful discrimination for exercising a privacy right.

96.5 State-law rights and response methods depend on statutory applicability thresholds and the person's residence. A jurisdiction-specific notice or Request Portal may supply additional information without reducing a mandatory right.

#### **97. Canadian Privacy Rights**

97.1 Where Canadian private-sector privacy law applies, an individual may request information about the existence, use and disclosure of Personal Information and may obtain access subject to lawful exceptions.

97.2 An individual may challenge the accuracy or completeness of Personal Information and request an appropriate correction or notation. Where appropriate, amended information may be transmitted to relevant recipients.

97.3 Consent may be withdrawn subject to legal or contractual restrictions and reasonable notice. CreamyPeach will explain material consequences, which may include loss of an optional feature or inability to continue a processing-dependent service.

97.4 Access will ordinarily be provided at no or minimal cost within the applicable period, generally 30 days under PIPEDA where it applies, subject to lawful extension and verification.

97.5 A Canadian individual may complain to CreamyPeach and, where applicable, to the Office of the Privacy Commissioner of Canada or the competent provincial privacy regulator.

## **98 Israeli Privacy Rights**

98.1 Where Israeli Privacy Protection Law applies, an individual may have rights to inspect Personal Data held about that person in a regulated database and to request correction or deletion where the information is inaccurate, incomplete, unclear or outdated, subject to applicable conditions and exceptions.

98.2 Requests involving information transferred from the EEA to Israel may also benefit from the protections described in the applicable Israeli regulations and the EU transfer framework.

98.3 A refusal may be challenged using the route available under Israeli law. CreamyPeach may coordinate with an Israeli Hosted Client or recipient that independently controls the relevant database.

98.4 Israeli rights will be administered through [privacy@creamypeach.com](mailto:privacy@creamypeach.com) unless a local controller or legally required contact must respond directly.

## **99. United Kingdom, Switzerland and Other Local Rights**

99.1 Individuals protected by the UK GDPR generally have rights corresponding to information, access, rectification, erasure, restriction, portability, objection and safeguards for solely automated significant decisions, subject to UK law.

99.2 Swiss individuals may request information about processing and, where applicable, correction, deletion, restriction or cessation of unlawful processing under the Swiss Federal Act on Data Protection.

99.3 Individuals in other jurisdictions may have additional rights, such as consent withdrawal, complaint, appeal, opt-out, correction or deletion. CreamyPeach will honor mandatory local rights where the law applies to its processing.

99.4 A country-specific addendum may clarify local terminology, deadlines, exemptions, regulator information or appeal rights. It supplements rather than silently narrows this global notice.

## **100. Non-Discrimination, Service Consequences and Financial Incentives**

100.1 CreamyPeach will not unlawfully discriminate against a person for exercising a privacy right.

100.2 CreamyPeach may be unable to provide a feature where the Personal Data are objectively necessary for that feature, such as authentication, payment processing, entitlements, personalized Chat Memory or a Hosted Client payout. Any difference will be reasonably related to the data and service.

100.3 Deleting an Account, withdrawing required processing or requesting restriction may terminate subscriptions, revoke access, interrupt pending services or prevent recovery of Wallet or entitlement records, subject to the Terms and mandatory consumer law.

100.4 CreamyPeach will not offer a price or service difference constituting a regulated financial incentive for Personal Data unless it first provides the notice, valuation and opt-in or withdrawal mechanism required by applicable law.

## **101. Privacy Questions, Internal Complaints and Appeals**

101.1 Privacy questions, complaints and request appeals may be sent to [privacy@creamypeach.com](mailto:privacy@creamypeach.com) with enough information to identify the issue and prior request or decision.

101.2 CreamyPeach will route the matter to personnel who were not solely responsible for the challenged decision where proportionate and will consider the law, evidence, account context, security, rights of others and prior communications.

101.3 A complaint may be combined with a billing, content, moderation, security or Hosted Client process, but the privacy component will be tracked and answered under applicable Data Protection Law.

101.4 CreamyPeach may preserve complaint records, evidence and communications for accountability, legal claims, safety and repeat-issue analysis under the retention schedule.

101.5 Using the internal route is encouraged because it may resolve the matter quickly, but it does not waive or unlawfully delay a right to contact a regulator or court.

## **102. Supervisory Authorities and Regulatory Complaints**

102.1 An individual protected by the GDPR has the right to lodge a complaint with a supervisory authority, particularly in the Member State of habitual residence, place of work or place of the alleged infringement.

102.2 Peachcream SRL's Romanian supervisory authority is the National Supervisory Authority for Personal Data Processing (ANSPDCP), 28-30 G-ral. Gheorghe Magheru Boulevard, Sector 1, postal code 010336, Bucharest, Romania; [anspdcp@dataprotection.ro](mailto:anspdcp@dataprotection.ro); [www.dataprotection.ro](http://www.dataprotection.ro).

102.3 ANSPDCP accepts complaints under its published procedure, including in Romanian or English. Its current forms and procedural requirements should be checked on its official website before submission.

102.4 UK individuals may complain to the Information Commissioner's Office; Canadian individuals to the Office of the Privacy Commissioner of Canada or a competent provincial regulator; Swiss individuals to the Federal Data Protection and Information Commissioner; Israeli individuals to the Privacy Protection Authority; and United States residents to the competent state regulator or privacy authority where applicable.

102.5 CreamyPeach asks individuals to contact it first where practical, but this is not a condition to exercise any direct regulatory right unless a particular authority's admissibility procedure requires prior contact.

### **103. Judicial Remedies, Representation and Compensation**

103.1 Nothing in this notice limits a non-waivable right to an effective judicial remedy against a controller, Processor or supervisory authority under applicable law.

103.2 A Data Subject may be entitled to mandate an eligible non-profit body, organization, consumer representative, lawyer or other representative to act under the conditions of applicable law.

103.3 A person who has suffered material or non-material damage from an infringement may have a statutory right to compensation. The existence and amount of any remedy are determined under applicable law and competent procedure.

103.4 Contractual dispute provisions do not override a mandatory privacy complaint, regulatory or judicial forum that cannot lawfully be waived.

### **104. Communications Following a Personal Data Breach**

104.1 CreamyPeach will assess each suspected Personal Data Breach as described in Clause 71 and will communicate with affected individuals without undue delay where the breach is likely to result in a high risk to their rights and freedoms or where another applicable law requires notice.

104.2 A breach communication will describe in clear language the nature of the breach, the contact point for further information, likely consequences and measures taken or proposed to address and mitigate the breach, to the extent known and legally permitted.

104.3 Notice may be provided by verified email, in-account message, prominent website communication, postal notice or another effective channel appropriate to the risk and available contact information.

104.4 Individual notice may not be required where effective measures such as strong encryption render the data unintelligible, later measures remove the high risk, or individual communication would involve disproportionate effort and an equally effective public communication is used, as permitted by law.

104.5 CreamyPeach may provide phased updates where all information is not available at once and may include specific protective steps such as password reset, payment monitoring, phishing caution or contact with a verification provider.

104.6 A security incident is not necessarily a Personal Data Breach, and not every Personal Data Breach legally requires individual notice. CreamyPeach will document its assessment and notify the competent authority where required.

### **105. Minors, Underage Data and Protective Deletion**

105.1 CreamyPeach is strictly for adults who meet the minimum age stated in the Terms and does not knowingly offer the Platform to minors.

105.2 If CreamyPeach learns that a minor submitted Personal Data or accessed the Platform, it may immediately restrict the Account, preserve narrowly necessary safety evidence, investigate, notify appropriate providers or authorities and delete or otherwise lawfully handle the data.

105.3 A parent or legal guardian may report suspected underage processing, but CreamyPeach will verify authority and will not disclose adult-service Account information to a third party without a lawful basis.

105.4 Reports involving possible child sexual abuse material, grooming, exploitation or trafficking will be handled under strict safety procedures and may be preserved and reported as required by law. An erasure request does not require destruction of evidence that must lawfully be preserved or reported.

105.5 CreamyPeach will not use known minors' Personal Data for marketing, Profiling, sale, sharing or adult-content personalization.

### **106. Changes to this Privacy Policy and New Processing**

106.1 CreamyPeach may update this Privacy Policy to reflect legal, regulatory, technical, security, vendor, product or business changes.

106.2 The current version and effective date will be displayed on the Website. CreamyPeach should maintain a reasonable version history or summary of material changes.

106.3 Material changes will be communicated through a prominent website notice, Account message, email or another appropriate channel before or when the change takes effect, as required by law.

106.4 If a change requires Consent or Explicit Consent, continued use alone will not substitute for the required affirmative action. The relevant feature may remain unavailable until a valid choice is made.

106.5 A notice update does not retroactively make unlawful processing lawful, expand a Hosted Client's access without proper role assessment, or override a prior opt-out or consent withdrawal.

106.6 Individuals should review layered notices for features introduced after the policy date, including new age-verification, biometric, AI, advertising or Hosted Client data flows.

#### **107. Controller, Privacy, DPO and Service Contacts**

107.1 Controller and operator: Peachcream SRL, operating CreamyPeach and creamypeach.com.

107.2 Registered office currently supplied: Soseaua lancelui nr. 53, Bucharest, Romania. The final public notice must reproduce the exact registered-office form and confirmed company identifiers shown in official records.

107.3 Privacy and Rights Requests: [privacy@creamypeach.com](mailto:privacy@creamypeach.com). General support: [support@creamypeach.com](mailto:support@creamypeach.com). Billing: [billing@creamypeach.com](mailto:billing@creamypeach.com). Security: [security@creamypeach.com](mailto:security@creamypeach.com). Formal legal notices: [legal@creamypeach.com](mailto:legal@creamypeach.com).

107.4 If Peachcream SRL appoints or is required to appoint a Data Protection Officer, the DPO's direct contact details will be published and communicated to the competent authority. Until then, [privacy@creamypeach.com](mailto:privacy@creamypeach.com) is the designated privacy contact route.

107.5 Because Peachcream SRL is established in Romania, it does not require an Article 27 EU representative for its own establishment. Any UK, Swiss or other representative legally required for applicable extraterritorial processing will be identified in a local addendum.

107.6 The company tax identifier, VAT status, DPO determination, local representative analysis and all email inboxes must be verified operationally before publication.