					Insert Registered Legal Entity Name Here							
Document number: PII22					Document Title: **Marketing Privacy and Cookies Policy**							
Version: 1.0		Effective Date: 01.01.2025			Document Owner:							
X	Policy		Standard		Procedure		Form		Register		Other	

Revision history				
Revision number	**Revision Date**	**Changes**	**Reviewed by**	**Process owner**

Approvals			
Name	**Title**	**Date**	**Signature**

Aligned with standards and regulations

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Documented marketing privacy evidence and operational control
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitoring, nonconformity and corrective action
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.4; Annex A.1.2.5; Annex A.1.2.9	Controller	Primary	Marketing purposes, lawful-basis linkage, consent and processing records
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Marketing processors and joint-controller responsibilities
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4; Annex A.1.3.5	Controller	Primary	Marketing notices, cookie notices and consent withdrawal information
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.10	Controller	Supporting	Objection and request-handling routing for direct marketing
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	Collection, processing and minimization for marketing and tracking
ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5	Conditional	Supporting	Transfer and disclosure routing for adtech and analytics
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Processor agreement, instruction, customer support and processor records
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4;	Processor	Supporting	Processor support for obligations, transfer and disclosure routing

	Annex A.2.5.5; Annex A.2.5.6			
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Protection of records and logging evidence for tracking changes
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Primary	Fairness, transparency, purpose limitation, minimization and accountability
GDPR	Article 6; Article 7	Controller	Primary	Lawfulness and consent conditions
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Transparent information and notices
GDPR	Article 21	Controller	Primary	Direct marketing objection and opt-out routing
GDPR	Article 24; Article 25; Article 26; Article 28; Article 30; Article 32	Both	Supporting	Accountability, design/default, joint controllers, processors, records and security support
GDPR	Article 44	Conditional	Referenced	International transfer routing for marketing vendors
ISO/IEC 29100:2020	Clause 5.1; Clause 5.8; Clause 5.9	Both	Primary	Consent and choice, transparency and participation
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Purpose, collection, minimization, use and disclosure limitation
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Accountability, information security and compliance
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Consent, purpose, collection, minimization, use/disclosure and participation controls

ISO/IEC TS 27560:2023	Clause 5.2; Clause 5.3; Clause 6.2; Clause 6.4	Controller	Supporting	Consent record and receipt structure where used

1. Scope

1.1 This policy defines mandatory privacy requirements for marketing, cookies, tracking technologies, analytics, advertising technology, audience segmentation, direct marketing, preference management, suppression, third-party tags, campaign review and related PII processing.

1.2 This policy applies to controller, joint controller, processor and subprocessor contexts.

1.3 Controller obligations apply where the organization determines marketing purposes and means.

1.4 Processor and subprocessor obligations apply only where the organization processes marketing, analytics, tracking or campaign-related PII under documented customer or upstream processor instructions.

1.5 This policy covers:

1.5.1 marketing processing inventory and purpose linkage;

1.5.2 consent and preference evidence for marketing and tracking;

1.5.3 cookie, tracking technology and tag governance;

1.5.4 marketing privacy notice and cookie notice records;

1.5.5 suppression, withdrawal and opt-out routing;

1.5.6 marketing vendor, analytics provider and adtech relationship governance;

1.5.7 international transfer routing for marketing vendors and platforms;

1.5.8 campaign review and monitoring evidence.

1.6 This policy does not create a separate cookie register, tag register, suppression register, marketing campaign register, analytics register, legal-advice workflow, committee, dashboard, form or non-canonical role.

1.7 This policy does not replace:

1.7.1 PII03 for processing inventory and lawful-basis ownership;

1.7.2 PII04 for general privacy notice governance;

1.7.3 PII05 for consent and preference management;

1.7.4 PII06 for PII principal rights request workflow;

1.7.5 PII07 for privacy risk assessment and DPIA methodology;

1.7.6 PII08 for privacy by design and default gates;

1.7.7 PII09 for general collection, use, disclosure and sharing controls;

1.7.8 PII10 for retention, deletion and disposal execution;

1.7.9 PII11 for accuracy and quality governance;

1.7.10 PII12 for processor, subprocessor and third-party lifecycle governance;

1.7.11 PII13 for international transfer mechanism assessment;

1.7.12 PII14 for PII security and access control architecture;

1.7.13 PII15 for PII incident and breach handling;

1.7.14 PII18 for PIMS monitoring, audit and improvement governance;

1.7.15 PII20 for child-specific marketing or tracking safeguards;

1.7.16 PII21 for AI, profiling and automated decision-making privacy controls;

1.7.17 PII23 for cloud PII processor controls where applicable.

2. Purpose

2.1 The purpose of this policy is to ensure that marketing, cookies, analytics, tracking and adtech processing are governed through clear purpose records, transparent notice, appropriate consent

or preference controls, suppression and withdrawal handling, third-party oversight, and audit-ready evidence.

2.2 This policy supports privacy accountability for B2C, analytics-heavy, adtech-enabled and consent-management-heavy environments without introducing non-canonical registers, roles or duplicative workflows.

3. Objectives

3.1 The objectives of this policy are to:

3.1.1 Ensure marketing and tracking purposes are recorded before processing begins.

3.1.2 Ensure consent, preference, suppression and withdrawal evidence is maintained in canonical evidence objects.

3.1.3 Ensure cookie notices and marketing notices are current, version-controlled and linked to processing records.

3.1.4 Ensure tracking technologies, tags, pixels, SDKs, analytics tools and adtech integrations are approved before production use.

3.1.5 Ensure marketing vendors, analytics providers and advertising partners are classified and governed through canonical relationship evidence.

3.1.6 Ensure opt-outs, objections, withdrawals and direct marketing complaints are routed consistently.

3.1.7 Ensure international transfer routing is performed for marketing vendors and analytics providers where applicable.

3.1.8 Ensure campaign and tracking controls are monitored, reviewed and improved using PIMS evidence.

4. Policy Statements

4.1 Marketing and Tracking Processing Inventory

4.1.1 [Controller] The Process Owner / Business Owner MUST record each marketing campaign, channel, processing purpose, PII category, audience source, lawful-basis linkage, tracking technology category, vendor or tag dependency, notice linkage, consent or preference dependency, retention linkage and transfer flag in REG02 before the campaign or tracking activity begins.

4.1.2 [Controller] The Privacy Lead / PIMS Manager MUST confirm that each marketing purpose in REG02 has current REG07 notice linkage and REG05 consent or preference linkage before campaign launch.

4.1.3 [Processor] The Process Owner / Business Owner MUST document customer-approved marketing purposes and customer instructions in REG02 or REG08 before processing marketing PII on behalf of a controller.

4.1.4 [Joint Controller] The Privacy Lead / PIMS Manager MUST record joint-controller responsibility allocation in REG08 before launching joint marketing, shared-audience, co-branded campaign or shared tracking activity.

4.1.5 [Conditional] The Privacy Lead / PIMS Manager MUST route marketing activities involving an international vendor, tag, analytics provider, advertising platform, audience transfer or data-sharing transfer to REG09 before go-live.

4.1.6 [Controller] The Process Owner / Business Owner MUST record suppression, exclusion or do-not-contact requirements associated with each marketing purpose in REG05 before activation.

4.2 Consent, Preference and Cookie Controls

4.2.1 [Controller] The Process Owner / Business Owner MUST identify whether consent, preference, objection, contractual instruction or another approved basis is required for each marketing channel and record the decision in REG02 and REG05 before collection or campaign use.

4.2.2 [Controller] The System Owner / Application Owner MUST configure non-essential cookies, tags, pixels, SDKs and similar tracking technologies to remain inactive until the required consent or preference state is available in REG05 before deployment.

4.2.3 [Controller] The System Owner / Application Owner MUST validate that consent or preference signals are not overwritten, bypassed or ignored during website, app, campaign or tag-manager changes and record validation evidence in REG05 or REG12 before release.

4.2.4 [Controller] The Process Owner / Business Owner MUST record consent, preference, withdrawal, suppression and version evidence in REG05 within one business day after capture, change or withdrawal.

4.2.5 [Processor] The System Owner / Application Owner MUST apply customer-provided consent, preference, suppression or instruction data to processor-managed marketing tools within the customer-agreed timeframe and record completion in REG05 or REG08.

4.2.6 [Conditional] The Privacy Lead / PIMS Manager MUST maintain consent receipt field mapping in REG05 before issuing consent receipts for marketing, cookie or tracking purposes.

[... Sections 4.3–8 are not included in this preview. Purchase the full document to access the complete policy content. ...]

9. Exceptions

9.1 [All] The Process Owner / Business Owner MUST request an exception in REG12 before using any non-standard marketing channel, tag, analytics configuration, preference mechanism or vendor where required evidence cannot be completed before launch.

9.2 [Conditional] The Data Protection Officer / Privacy Advisor MUST review a marketing privacy exception request in REG12 before approval when the exception affects consent, children, employees, sensitive audiences, cross-border transfer, profiling or material tracking expansion.

9.3 [All] Top Management MUST approve high-risk or material marketing privacy exceptions in REG12 before the exception becomes effective.

9.4 [All] The Privacy Lead / PIMS Manager MUST set an expiry date, remediation owner and review date in REG12 for every approved marketing privacy exception before approval.

10. Enforcement

10.1 [All] The Privacy Lead / PIMS Manager MUST suspend or block a marketing activity in REG12 when required REG02, REG05, REG07, REG08 or REG09 evidence is missing before launch or continued use.

10.2 [All] The System Owner / Application Owner MUST disable unapproved tags, trackers, pixels, SDKs or campaign data flows within one business day after an enforcement decision and record completion in REG08 or REG12.

10.3 [All] The Vendor / Procurement Owner MUST block onboarding, renewal or expansion of a marketing vendor, analytics provider or advertising platform when required REG08 or REG09 evidence is missing before processing begins or continues.

10.4 [All] The Process Owner / Business Owner MUST stop campaign use of affected PII within one business day after a confirmed preference, suppression, notice or vendor control failure and record completion in REG05 or REG12.

10.5 [All] The Internal Audit / Compliance Reviewer MUST verify corrective action effectiveness for major or repeated marketing privacy nonconformities in REG12 within 60 days after corrective action closure.

11. Review and Maintenance

11.1 [All] The Privacy Lead / PIMS Manager MUST review this policy in REG12 annually and within 30 days after a material change to marketing, cookies, tracking, analytics, adtech or consent-management requirements.

11.2 [Controller] The Process Owner / Business Owner MUST review REG02 marketing processing records and REG05 preference dependencies at least quarterly and within 30 days after a material campaign change.

11.3 [Controller] The Privacy Lead / PIMS Manager MUST review REG07 marketing notice and cookie notice records at least annually and within 30 days after a material notice, tracking or preference change.

11.4 [All] The Vendor / Procurement Owner MUST review REG08 marketing vendor, tag, analytics and advertising platform records at least annually and before renewal.

11.5 [Conditional] The Privacy Lead / PIMS Manager MUST update REG09 transfer routing within 15 business days after an identified marketing vendor, analytics provider or hosting-location change.

11.6 [All] Top Management MUST approve material revisions to this policy in REG12 before publication.

12. Related Policies

12.1 This policy is supported by the following related policies:

12.2 PII01 - Privacy Information Management System Policy

12.3 PII02 - Privacy Roles, Responsibilities and Accountability Policy

12.4 PII03 - PII Processing Inventory and Lawful Basis Policy

12.5 PII04 - Privacy Notice and Transparency Policy

12.6 PII05 - Consent and Preference Management Policy

12.7 PII06 - PII Principal Rights Management Policy

12.8 PII07 - Privacy Risk Assessment and DPIA Policy

12.9 PII08 - Privacy by Design and Default Policy

12.10 PII09 - PII Collection, Use, Disclosure and Sharing Policy

12.11 PII10 - PII Retention, Deletion and Disposal Policy

12.12 PII11 - PII Accuracy and Quality Policy

12.13 PII12 - Processor, Subprocessor and Third-Party Privacy Management Policy

12.14 PII13 - International PII Transfer Policy

12.15 PII14 - PII Security and Access Control Policy

12.16 PII15 - PII Incident and Breach Management Policy

12.17 PII17 - PIMS Documented Information and Evidence Management Policy

12.18 PII18 - PIMS Monitoring, Audit and Improvement Policy

12.19 PII19 - Employee Privacy Policy

12.20 PII20 - Children's Privacy Policy

12.21 PII21 - AI and Automated Decision-Making Privacy Policy

12.22 PII23 - Cloud PII Processor Policy

13. Reference Standards and Frameworks

13.1 This policy is mapped to the following standards and regulations. The mapping explains how the policy supports the cited requirements and identifies the internal clauses that implement or support them.

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.4; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1; 7.2; 7.6; 11.1].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.3.6; 4.5.5; 4.6.5; 4.7.4; 6.1; 6.5; 8.1; 8.2; 8.3; 8.4; 8.5; 10.5; 11.1].

13.4 ISO/IEC 27701:2025 - Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.4; Annex A.1.2.5; Annex A.1.2.9. Addressed by clauses [4.1.1; 4.1.2; 4.1.6; 4.2.1; 4.2.4; 4.2.6; 4.5.1; 4.7.2; 7.1; 11.2].

13.5 ISO/IEC 27701:2025 - Annex A.1.2.7; Annex A.1.2.8. Addressed by clauses [4.1.4; 4.4.2; 4.4.3; 4.4.5; 5.6; 6.4; 7.5; 11.4].

13.6 ISO/IEC 27701:2025 - Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4; Annex A.1.3.5. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 7.3; 11.3].

13.7 ISO/IEC 27701:2025 - Annex A.1.3.6; Annex A.1.3.10. Addressed by clauses [4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 7.2].

13.8 ISO/IEC 27701:2025 - Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5. Addressed by clauses [4.1.1; 4.2.2; 4.4.4; 4.5.1; 4.5.2; 4.5.4; 4.5.5; 4.7.2; 7.2].

13.9 ISO/IEC 27701:2025 - Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5. Addressed by clauses [4.1.5; 4.4.3; 4.4.6; 7.5; 11.5].

13.10 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.3; 4.2.5; 4.3.4; 4.4.5; 7.4].

13.11 ISO/IEC 27701:2025 - Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.2.5; 4.3.4; 4.4.6; 4.6.3; 7.4; 7.5].

13.12 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.25. Addressed by clauses [4.2.3; 4.4.4; 4.7.1; 4.7.3; 5.7; 7.2; 10.2].

13.13 GDPR - Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(2). Addressed by clauses [4.1.1; 4.1.2; 4.1.6; 4.5.1; 4.5.2; 4.7.2; 8.1].

13.14 GDPR - Article 6; Article 7. Addressed by clauses [4.2.1; 4.2.2; 4.2.4; 4.2.6; 4.6.2; 7.2].

13.15 GDPR - Article 12; Article 13; Article 14. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.5; 11.3].

13.16 GDPR - Article 21. Addressed by clauses [4.5.2; 4.6.1; 4.6.2; 4.6.4; 8.3].

13.17 GDPR - Article 24; Article 25; Article 26; Article 28; Article 30; Article 32. Addressed by clauses [4.1.3; 4.1.4; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 4.7.3; 5.6; 5.7; 6.2; 6.4; 8.4; 10.3].

13.18 GDPR - Article 44. Addressed by clauses [4.1.5; 4.4.6; 7.5; 11.5].

13.19 ISO/IEC 29100:2020 - Clause 5.1; Clause 5.8; Clause 5.9. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.3; 4.6.1; 4.6.2].

13.20 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.5.1; 4.5.2; 4.5.4; 4.7.2].

13.21 ISO/IEC 29100:2020 - Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.3.6; 4.5.5; 4.6.5; 4.7.1; 4.7.3; 4.7.4; 6.1; 8.5; 10.5].

13.22 ISO/IEC 29151:2022 - Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10. Addressed by clauses [4.2.1; 4.2.2; 4.2.4; 4.5.1; 4.5.2; 4.6.1; 4.6.2; 7.2].

13.23 ISO/IEC TS 27560:2023 - Clause 5.2; Clause 5.3; Clause 6.2; Clause 6.4. Addressed by clauses [4.2.4; 4.2.6; 7.1; 7.2].