

MSPA and Global Privacy Platform (GPP) Integration and Rollout Guide

For Ad Tech Engineering Teams - Version 1.0

1. Purpose

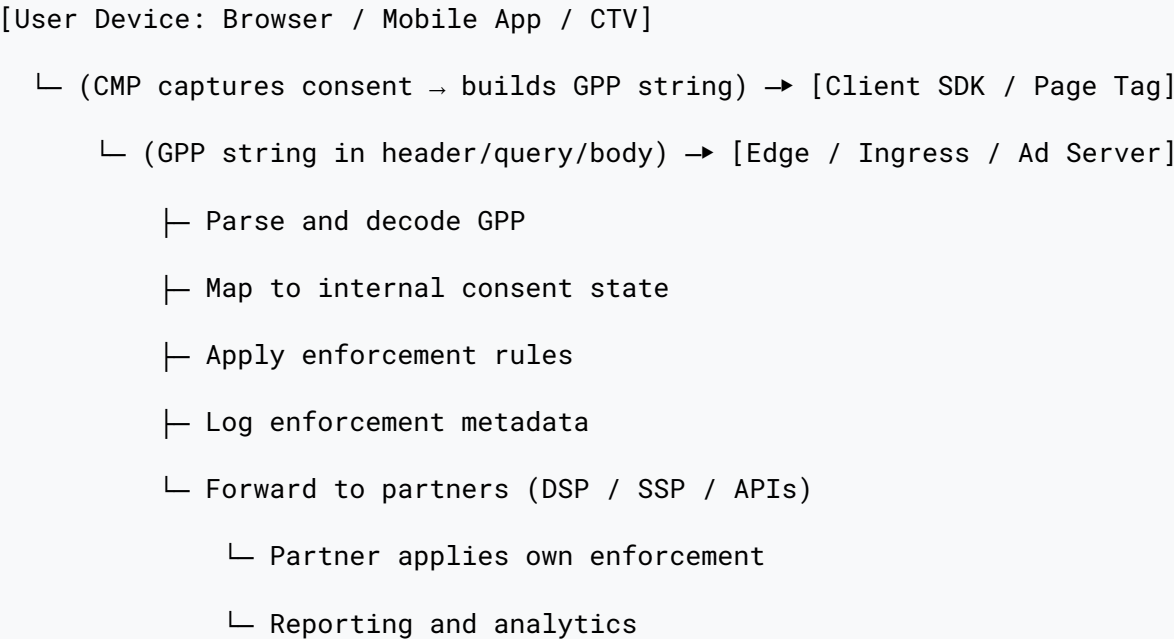
This guide provides engineering, ad operations, product, and compliance teams with a practical framework for implementing the [IAB Multi-State Privacy Agreement \(MSPA\)](#) and the [Global Privacy Platform \(GPP\)](#) across ad tech systems. It merges the IAB specifications with company-specific enforcement rules, integration points, operational policies, and testing procedures to ensure privacy compliance at scale.

2. System Architecture and Data Flows

Overview

Privacy compliance requires end-to-end visibility into how signals are generated, transmitted, and enforced.

Flow Diagram (Text Representation)



Key Integration Points

- **Client SDK or Page Tag:** Captures CMP consent output and attaches GPP string to outgoing requests.
- **Ad Server / Ingress Layer:** Validates GPP, decodes, and maps to internal enforcement rules.
- **Targeting Engine:** Applies audience and data restrictions.
- **Partner APIs:** Ensures GPP is included in OpenRTB payloads for DSP/SSP compatibility.
- **Data Pipeline:** Stores decoded consent data and enforcement actions for auditing.

3. GPP Signal Integration

- GPP strings are **base64-encoded** and separated by ~ for each jurisdiction.

Example:

- DBABBg~BUoAAABg.Q
- DBABBg = Header section
- BUoAAABg.Q = California-specific section

Requirements:

- Attach GPP to bid requests in `regs.ext.gpp` and `user.ext.gpp` per [OpenRTB 2.6](#).
- Immediately update GPP values if user consent changes.

4. Enforcement Policies

A. Mapping Bits to Internal Flags

- SaleOptOut** → Internal flag: disable behavioral targeting
- ShareOptOut** → Internal flag: block third-party sharing
- GPC flag** → Internal flag: enforce global strict opt-out
- MSPA Transaction** → Internal flag: apply contractual rules

B. Enforcement Logic

flowchart Top-Down

A [Start] --> B {Is GPC = 1?}
B -- Yes --> C [Apply full opt-out (block targeting, sharing, PII)]
B -- No --> D {Is SaleOptOut = 1?}
D -- Yes --> E [Disable behavioral targeting Strip PII → Contextual ads only]
D -- No --> F {Is ShareOptOut = 1?}
F -- Yes --> G [Block sharing with third parties (no cookie/device syncs)]
F -- No --> H {Is MSPA Transaction = True?}
H -- Yes --> I [Apply MSPA-specific contractual rules]
H -- No --> J [Allow normal processing]

What the letters stand for in the Mermaid flowchart

A = Start
B = Check if GPC = 1
C = Enforcement when GPC = 1 (strict opt-out)
D = Check if SaleOptOut = 1
E = Enforcement when SaleOptOut = 1 (contextual only)
F = Check if ShareOptOut = 1

G = Enforcement when ShareOptOut = 1 (no third-party sharing)
H = Check if MSPA Transaction = True
I = Enforcement when MSPA = True (apply contractual rules)
J = Normal processing (no restrictions triggered)

C. Enforcement Text Cases Matrix

Enforcement Matrix with Example GPP Strings						
Case	GPC	Sale OptOut	Share OptOut	MSPA Transaction	Enforcement Result	Example GPP String*
1	1	X	X	X	Full opt-out (block targeting, sharing, PII)	DBABBg~BUoAAAAAA
2	0	1	X	X	Contextual ads only (disable targeting, strip PII)	DBABBg~BUoAAABg.Q
3	0	0	1	X	No third-party sharing (disable syncs)	DBABBg~BUoAAACg.Q
4	0	0	0	1	Apply MSPA contractual rules	DBABBg~BUoAAADA.Q
5	0	0	0	0	Allow normal processing	DBABBg~BUoAAAAg.Q

Notes:

- X = “N /A” - Not Applicable
- Always enforce the most restrictive rule when signals conflict.

5. Compliance and Testing Procedures

Validation

- Use official or community-developed GPP validators.
- Maintain automated unit tests for all known consent combinations.

Monitoring

- Log decoded GPP values at all key processing points.
- Trigger alerts for malformed, missing, or inconsistent signals.

Manual QA

- Periodically sample and review live traffic.
- Cross-check compliance with the legal and privacy teams.

6. Rollout and Versioning

- **Phases:** Development → Pilot → Full rollout → Post-rollout audit.
- **Version Control:** Track which IAB GPP specification version is supported; ensure backward compatibility where required.

7. Logging and Audit

- Store decoded consent flags with enforcement outcomes.
 - Mask or remove PII when SaleOptOut = 1 or GPC = 1.
 - Retain logs according to compliance schedules.
 - Maintain audit-ready queries for regulatory requests.
-

8. Technical Appendix

A. Full System Sequence Diagram (Mermaid Syntax)

sequenceDiagram

```
User->>CMP: User sets privacy preferences
CMP->>SDK: Returns GPP string
SDK->>AdServer: Sends ad request with GPP
AdServer->>AdServer: Decode and map to consent flags
AdServer->>Targeting: Apply restrictions
Targeting->>Partner: Send bid request with GPP
Partner->>AdServer: Return creative / no-bid
AdServer->>User: Serve creative
AdServer->>Logs: Store decoded GPP and enforcement action
```

B. Example OpenRTB Bid Request with GPP

```
{
  "id": "abc-123",
  "regs": {
    "ext": {
      "gpp": "DBABBg~BUoAAABg.Q",
      "gpp_sid": [7]
    }
  },
  "user": {
    "ext": {
      "gpp": "DBABBg~BUoAAABg.Q"
```

```

    }
  },
  "imp": [
    { "id": "1", "banner": { "w": 300, "h": 250 } }
  ],
  "site": { "domain": "example.com" }
}

```

C. Sample Enforcement Policy JSON

```

{
  "sale_opt_out": {
    "strip_pii": true,
    "disable_audiences": true
  },
  "share_opt_out": {
    "disable_partner_syncs": true
  },
  "gpc": {
    "override_other_signals": true
  }
}

```

D. Useful Tools and Resources

- [IAB GPP Validator](#)
- [MSPA Technical Signaling Guidelines](#)
- [IAB Multi-State Privacy Agreement Overview](#)
- [IAB GPP Specification Overview](#)

9. QA Test Cases

Objective: Validate that system behavior matches enforcement requirements when processing GPP consent strings across all supported scenarios.

A. Test Environment Setup

- Deploy the latest build with GPP string parsing enabled.
- Enable **debug logging** for `regs.ext.gpp` and `user.ext.gpp`.
- Use the official [IAB Tech Lab GPP Encoder/Decoder](#) to generate test strings.
- Ensure bidstream inspection tools (e.g., Charles Proxy, Fiddler, or internal log viewer) are configured.

B. Test Cases Matrix

Case	Signal Combination	Expected System Behavior	QA Validation Steps
1. Full Opt-Out (GPC=1)	GPC=1 (SaleOptOut/ShareOptOut ignored)	- Block all behavioral targeting - Strip PII from bidstream - Contextual ads only	1. Send request with GPC=1 string. 2. Inspect bidstream → confirm no PII or IDs. 3. Confirm only contextual ads are returned.
2. Sale Opt-Out	SaleOptOut=1, GPC=0	- Disable behavioral targeting - Strip PII - Allow contextual ads	1. Send request with SaleOptOut=1 string. 2. Confirm no IDs or user data in bidstream. 3. Validate contextual-only creative returned.
3. Share Opt-Out	ShareOptOut=1, SaleOptOut=0, GPC=0	- Allow behavioral targeting - Block cookie/device syncs	1. Send request with ShareOptOut=1 string. 2. Confirm no sync pixels fired. 3. Confirm ads can still target segments.
4. MSPA Transaction	MSPA Transaction=1, SaleOptOut=0, ShareOptOut=0, GPC=0	- Apply MSPA-specific contractual handling	1. Send request with MSPA Transaction flag set. 2. Confirm partner payload includes MSPA notice. 3. Validate downstream systems flag transaction as covered.
5. Normal Processing	All signals = 0	- Allow standard targeting - Syncs allowed - PII included where permitted	1. Send request with default GPP string. 2. Confirm bidstream includes IDs. 3. Validate behavioral ads return.

C. Negative Testing

- **Malformed GPP String:** Ensure system rejects or defaults to “most restrictive.”
- **Conflicting Flags:** Example → GPC=1 + SaleOptOut=0 → Must apply **strictest rule (GPC=1)**.
- **Missing GPP Section:** Default to most restrictive interpretation.

D. Logging and Verification

- For each test, confirm logs show:
 - Raw GPP string
 - Decoded flag values (SaleOptOut, ShareOptOut, GPC, MSPA)
 - Enforcement action taken
- Log format should allow compliance/legal to audit enforcement.

E. Acceptance Criteria

- All test cases pass without PII leakage when opt-out is signaled.
- Enforcement matches **decision tree** and **matrix** rules.
- Conflicts always resolve to the **most restrictive**.
- Logs are accurate and audit-ready.

10. QA Checklist – MSPA and GPP Enforcement

Core Test Cases

- ☐ **Case 1 – GPC=1** → Confirm contextual-only ads, no IDs/PII in bidstream.
- ☐ **Case 2 – SaleOptOut=1** → Confirm contextual ads only, no targeting, no PII.
- ☐ **Case 3 – ShareOptOut=1** → Confirm behavioral ads allowed, but no cookie/device syncs.
- ☐ **Case 4 – MSPA Transaction=1** → Confirm MSPA contractual handling applied in payload/logs.
- ☐ **Case 5 – Normal Processing (all 0)** → Confirm standard targeting, IDs present, syncs allowed.

Negative Tests

- ☐ **Malformed GPP String** → Confirm system defaults to most restrictive.
- ☐ **Conflicting Flags (e.g., GPC=1 + SaleOptOut=0)** → Confirm strictest rule enforced (full opt-out).
- ☐ **Missing GPP Section** → Confirm system defaults to most restrictive.

Logging Verification

- ☐ Each test logs the raw GPP string.
 - ☐ Each test logs decoded flags (SaleOptOut, ShareOptOut, GPC, MSPA).
 - ☐ Each test logs the enforcement action taken.
 - ☐ Logs are audit-ready (timestamped, tied to request ID).
-

11. Supported Levels

A. GPP State-Level Support + MSPA US National Section

As of early 2024, GPP supports privacy strings for the following five states:

- California
- Colorado
- Connecticut
- Utah
- Virginia

B. Expanded Coverage (added in August 2024)

- Delaware
- Indiana
- Iowa
- Kentucky
- Maryland
- Michigan
- Montana
- New Hampshire
- Nebraska
- New Jersey
- Oregon
- Rhode Island
- Tennessee
- Texas

Reference: [IAB Tech Lab](#)

