



COGNITIVE MODE OPERATING SYSTEM STANDARDS BOARD

CMOS-SB Standard 0004

Emotional Data Consent & Privacy Standard

EDCPS v1.0 | Ratified Date: July 26, 2026 | Status: **Active - Public Comment** | Next Review: July 26, 2027

Field	Value
Standard ID	CMOS-SB-1004
Short Name	EDCPS
Version	1.0
Governance Spine Position	Pillar 4 of 5 — Consent & Privacy
Issued by	CMOS-SB Standards Committee
Ratified by	Founding Council, July 26, 2026
Published	June 9, 2026 (formal public comment period 7/26/26 -8/26/26)
Author / Architect	Isabelle Anne Thompson
Theoretical Basis	Emotional Epidemiology / Cognitive Mode OS Theory
Publication Set Item	Item 9 of the CMOS-SB Publication Set
Prerequisite Standards	EISS (1001) / CMSS (1002) / ETDS (1003)

Governance Note *EDCPS mandates explicit, informed, and granular consent for any emotional data collection, processing, or retention. Emotional surveillance is prohibited. EDCPS compliance requires prior full compliance with EISS, CMSS, and ETDS.*

Cognitive Mode OS™ is a trademark of Isabelle Anne Thompson / Sugar Sands Publishing LLC. All rights reserved.

Table of Contents

1.	Purpose and Scope	3
2.	Theoretical Foundations	4
3.	Emotional Data Classification Framework	5
4.	Consent Architecture Requirements	6
5.	Informed Consent Standards	7
6.	Consent Withdrawal and User Rights	8
7.	Data Minimization Requirements	9
8.	Retention and Deletion Standards	10
9.	Third-Party Sharing Restrictions	11
10.	Special Population Protections	12
11.	Prohibited Practices	13
12.	Compliance Checklist	14

PREREQUISITE NOTICE

EDCPS compliance requires prior demonstrated compliance with **CMOS-SB Standard 1002 — Emotional Intelligence and Sensitivity Standard (EISS)**. Systems that have not achieved EISS certification may not represent themselves as EDCPS-compliant. The consent and privacy protections established herein presuppose the emotional intelligence infrastructure defined in EISS.

1. Purpose and Scope

1.1 Purpose

The Emotional Data Consent and Privacy Standard (EDCPS) establishes binding requirements governing how systems subject to CMOS-SB jurisdiction collect, process, store, use, and share **emotional data** — defined as any data derived from, inferring, or modeling the emotional state, cognitive mode, attentional pattern, affective signal, or psychological profile of a human user.

EDCPS establishes a **consent-first architecture** that treats emotional data as a category of heightened sensitivity, requiring affirmative, informed, and withdrawable consent before any collection or use may commence. This standard recognizes that emotional data occupies a uniquely intimate domain: it reflects the interior life of the person, carries significant potential for misuse, and — when aggregated or deployed at scale — carries measurable population-level consequences that extend beyond any individual interaction.

The purpose of EDCPS is therefore threefold:

1. To protect the dignity, autonomy, and psychological privacy of individual users by ensuring they retain meaningful, ongoing control over their emotional data;
2. To establish structural safeguards that prevent systems from exploiting emotional data in ways that undermine user welfare, cognitive freedom, or informed decision-making; and
3. To define enforceable standards that hold systems accountable for the full lifecycle of emotional data — from collection through deletion.

EDCPS is Pillar 4 of the CMOS-SB Governance Spine, positioned to operationalize the consent and privacy commitments that the broader standards framework establishes as foundational to ethical system design.

1.2 Scope

EDCPS applies to **all systems within CMOS-SB jurisdiction**, including but not limited to: artificial intelligence systems, digital platforms, adaptive learning environments, health and wellness applications, productivity tools, communication systems, and any other technology that collects or processes information about how users feel, think, or cognitively engage.

The following scope principles govern EDCPS applicability:

Scope Dimension	EDCPS Position
EISS Prerequisite	EDCPS compliance requires prior EISS compliance. Systems must demonstrate active EISS certification before EDCPS obligations attach.
Inferred Emotional Data	Inferred emotional data is subject to all EDCPS requirements equally with directly collected data. The manner of derivation does not reduce the protection obligation.
Aggregate and Anonymized Data	Aggregate and anonymized emotional data (Tier C) remain subject to reduced but still-present EDCPS requirements as defined in Section 3.
Third-Party Processors	Any third party that processes emotional data on behalf of a subject system inherits all applicable EDCPS obligations through contractual binding as required by Section 9.
Geographic Applicability	EDCPS applies wherever a subject system operates, regardless of the user's geographic location. Where local law imposes higher standards, local law governs.

Systems must demonstrate active compliance with all consent, minimization, retention, sharing, and prohibited practices requirements contained herein. Compliance is not a one-time certification event but an ongoing operational obligation subject to continuous audit and periodic renewal.

2. Theoretical Foundations

2.1 Grounding in Cognitive Mode OS Theory

EDCPS is grounded in **Cognitive Mode OS Theory**, which proposes that human psychological functioning operates through a set of cognitive modes — stable configurations of attention, affect, and engagement that shape how individuals perceive, process, and respond to information. These modes are not fixed traits but dynamic states that are influenced by context, interaction, and the emotional content of the environment in which the individual is operating.

Emotional data — the record of what mode an individual is in, how they are feeling, and what affective signals they are emitting — therefore constitutes a map of the individual's interior operating state at a given moment. This map has extraordinary value for systems seeking to optimize engagement,

productivity, or behavior. But that same value is precisely what makes its protection essential: a system with access to a user's emotional map has access to the most intimate lever of influence available.

2.2 Emotional Epidemiology and Population-Level Sensitivity

EDCPS is further informed by the principles of **Emotional Epidemiology**, which examines how emotional states — and the conditions that produce them — propagate across populations. Just as infectious disease epidemiology studies transmission dynamics, Emotional Epidemiology examines the conditions under which emotional states spread, cluster, and amplify across connected individuals and systems.

Emotional data is uniquely sensitive for three interconnected reasons:

4. **Interior Intimacy:** Emotional data reflects the interior psychological state of the individual — it is among the most personal information that can be known about a person, more intimate in many respects than financial or medical data because it describes not what happened to the person but who they are in a given moment.
5. **Influence Capacity:** Emotional data can be used to identify and exploit moments of heightened susceptibility, shaping behavior, purchasing decisions, political attitudes, and social engagement in ways the user has not chosen and may not be aware of.
6. **Population-Scale Harm:** When emotional data is processed at population scale — across millions of users simultaneously — its misuse can produce measurable shifts in collective mood, susceptibility, and behavior that constitute a form of psychological harm to entire communities.

2.3 The S-R-C Model and Consent as Structural Safeguard

The **Susceptibility-Response-Contagion (S-R-C) Model**, developed within Cognitive Mode OS Theory, establishes that systems operating with access to emotional data have direct capacity to affect both individual Susceptibility (how vulnerable a user is to influence in a given cognitive mode) and population-level Transmission dynamics (how quickly emotional states and behavioral patterns propagate across connected users).

This positions consent not merely as a user preference mechanism or a procedural compliance checkbox, but as a **structural safeguard with population-level implications**. When users can meaningfully consent to or refuse emotional data collection, they exercise a form of epidemiological

agency — they determine whether their interior state enters a system's model, and under what conditions. Consent, in this framework, is a circuit breaker in the S-R-C transmission chain.

FOUNDATIONAL PRINCIPLE

The EDCPS consent-first architecture is not merely a user experience requirement. It is a structural intervention in the dynamics through which emotional data, at scale, can be used to influence population-level susceptibility and behavior. Consent architecture is, in the Cognitive Mode OS framework, a form of public health infrastructure.

3. Emotional Data Classification Framework

EDCPS establishes a three-tier classification framework for emotional data. All emotional data processed by systems within CMOS-SB jurisdiction must be classified into one of the following tiers prior to any collection, processing, storage, or sharing. Tier classification determines applicable consent requirements, retention limits, and sharing restrictions as specified in Sections 4 through 9.

Where data could reasonably be classified into more than one tier, the **higher-sensitivity tier governs**. Tier reclassification requires documented review and fresh consent if the new classification is higher than the original.

Tier	Name	Definition	Sensitivity Level	Examples
Tier A	Direct Emotional Signals	Explicitly expressed emotional content collected directly from the user's own expressive output.	Highest	Text explicitly expressing emotion; voice tone and prosody data; facial expression data; self-reported mood or emotional state; physiological signals (heart rate, galvanic skin response) when used to infer emotional state.
Tier B	Inferred Emotional States	Emotional data derived through inference from behavioral, interaction,	High	Emotional states inferred from typing speed, pause patterns, or interaction timing; engagement depth as a proxy for

Tier	Name	Definition	Sensitivity Level	Examples
		or engagement patterns rather than direct expression.		emotional investment; content consumption patterns used to model emotional state; session behavior interpreted as evidence of distress or elevated arousal.
Tier C	Aggregate Emotional Indicators	Population-level or anonymized emotional trend data from which individual identification has been removed through documented anonymization processes.	Moderate	Aggregate sentiment trends across user populations; anonymized cohort emotional profiles; population-level cognitive mode distribution data; de-identified emotional response patterns used for system design.

3.1 Tier-Specific Obligation Summary

Obligation	Tier A	Tier B	Tier C
Affirmative consent required before collection	Yes — Mandatory	Yes — Mandatory	Yes — Required at cohort level
Layered consent by data category	Required	Required	Recommended
Maximum default retention	90 days	180 days	365 days
Third-party sharing without explicit consent	Prohibited	Prohibited	Restricted — processor agreements required
User right of deletion	Full — mandatory	Full — mandatory	Cohort-level — as technically feasible
Re-identification prohibition	Applies	Applies	Applies — expressly

3.2 Classification Documentation Requirements

Systems must maintain a current **Emotional Data Inventory** that documents: (a) each category of emotional data collected; (b) its assigned tier; (c) the basis for that tier assignment; (d) the consent mechanism applied; and (e) the retention schedule in force. This inventory must be made available to

the CMOS-SB Standards Committee upon audit request and must be reviewed and re-certified no less than annually.

4. Consent Architecture Requirements

4.1 Consent-First Principle

No emotional data collection, inference, or processing of any kind may commence before **affirmative informed consent** has been obtained from the user in accordance with the standards set forth in Section 5. The consent-first principle is absolute: systems may not collect emotional data and seek retroactive consent, may not treat user silence or inaction as consent, and may not use technical architecture to make consent refusal practically difficult while consent acceptance is frictionless.

The consent-first principle applies equally to:

- Initial data collection at the point of first interaction;
- The expansion of emotional data collection to new categories or tiers;
- The application of emotional data to new purposes not disclosed at the time of original consent;
- The transfer of emotional data processing to new systems, processors, or organizational entities.

4.2 Layered Consent Architecture

Systems must implement **layered consent structures** that disaggregate emotional data collection into meaningful categories and allow users to consent to or refuse each tier and sub-category independently. Bundled consent — in which the user is asked to consent to emotional data collection as an undifferentiated condition of using a service — does not satisfy EDCPS requirements.

A compliant layered consent architecture must include, at minimum:

7. **Tier-Level Consent:** Separate consent decisions for Tier A, Tier B, and Tier C data as defined in Section 3;
8. **Purpose-Level Consent:** Consent decisions segmented by the purpose for which each data category will be used (e.g., service personalization vs. system improvement vs. research);

9. **Sharing-Level Consent:** Separate consent for any sharing of emotional data with third parties, as required by Section 9;
10. **Granular Opt-In:** Each consent layer must default to off (not collected) and require a positive user action to activate.

4.3 Consent Records

All consent decisions — whether affirmative consent, refusal, or withdrawal — must be recorded in a **Consent Ledger** with the following attributes:

Ledger Field	Requirement
User Identifier	Pseudonymized identifier linking consent record to the relevant user account
Consent Decision	Affirmative consent, refusal, or withdrawal — per tier and per purpose
Timestamp	Date and time of consent decision, recorded to the minute, in UTC
Version Reference	Version number of the consent disclosure document presented at time of decision
Method of Consent	Description of the interface mechanism through which consent was obtained
Consent Scope	Precise description of the data categories and purposes covered by the consent decision
Audit Accessibility	Records must be accessible to CMOS-SB auditors and available to users upon request

Consent records must be retained for a minimum of three (3) years from the date of the most recent consent decision, even after all associated emotional data has been deleted.

4.4 Re-Consent Requirements

Existing consent cannot be extended to cover new uses, new data categories, new processing purposes, or new sharing arrangements. **Material changes to data practices require fresh consent** obtained in accordance with Section 5 before the new practices may commence. A change is material if it:

- Adds a new tier of emotional data not previously collected;
- Introduces a new purpose for existing emotional data collection;
- Expands sharing to a new category of third party;

- Extends the retention period for any tier of emotional data;
- Materially changes the nature of how emotional data is processed or modeled.

5. Informed Consent Standards

Consent is **informed** under EDCPS only when the user has been provided with complete, accurate, and comprehensible information sufficient to make a genuine and autonomous decision about whether to permit emotional data collection. The following elements are mandatory components of every EDCPS-compliant consent disclosure.

5.1 Required Disclosure Elements

#	Disclosure Element	Standard
1	What is collected	Plain language description of the specific categories and tiers of emotional data to be collected, with examples sufficient for a non-technical user to understand what is being captured.
2	How it is collected	Description of the collection mechanism — whether direct input, inference from behavior, physiological signal, or other method — for each category of emotional data.
3	What it is used for	Specific, concrete statement of each purpose for which the emotional data will be used. General statements such as "to improve our service" without further specification do not satisfy this requirement.
4	Who has access	Identification of internal teams and roles with access to emotional data, and description of any third-party access by category of recipient.
5	Retention period	Clear statement of how long each tier of emotional data is retained before mandatory deletion, including what triggers the retention clock.
6	Consequences of refusal	Honest disclosure of what, if anything, the user will not be able to access or use if they decline consent. Denial of core service as a consequence of refusing emotional data consent is prohibited — see Section 11.
7	Available alternatives	Description of any alternative service pathways available to users who decline emotional data collection, including any limitations of those alternatives.

#	Disclosure Element	Standard
8	User rights	Plain language summary of the user's rights under Section 6: access, correction, deletion, portability, and withdrawal.
9	Contact and redress	Contact information for the system's privacy function, and description of how the user may file a complaint or exercise their rights.

5.2 Plain Language Requirement

Consent disclosures must be written at a language level accessible to a general adult population.

Consent text must not rely on legal terminology, technical jargon, or complex sentence structures that obscure the practical meaning of the disclosure. Systems are encouraged to conduct readability testing to verify comprehension prior to deployment of consent language.

5.3 Void Consent

Consent obtained through any of the following mechanisms is **void under EDCPS** and does not constitute a lawful basis for emotional data collection:

- **Dark patterns:** Interface designs that obscure the refusal option, make refusal require more steps than consent, or use visual hierarchy to steer users toward consent;
- **Pre-checked boxes:** Any consent mechanism in which the affirmative consent option is selected by default;
- **Misleading framing:** Consent language that misrepresents what is being collected, how it will be used, or the consequences of refusal;
- **Bundled consent:** Consent to emotional data collection bundled into general terms of service acceptance without clear, prominent, separate disclosure;
- **Coerced consent:** Consent obtained by conditioning access to a core service on agreement to emotional data collection where that collection is not strictly necessary for the service to function.

ENFORCEMENT NOTE

A finding that consent was obtained through a void mechanism does not merely invalidate the consent for future use — it renders all emotional data collected under that consent subject to immediate deletion obligations under Section 8, regardless of the data's retention age or the cost of deletion.

6. Consent Withdrawal and User Rights

Users retain ongoing rights with respect to their emotional data throughout its entire lifecycle. These rights are not waivable through consent at the time of collection: a user may not consent away their future right to withdraw, access, correct, delete, or export their emotional data. Any provision in a consent instrument that purports to extinguish these rights is void under EDCPS.

6.1 Right of Withdrawal

Users must be able to **withdraw consent at any time**, without penalty and without being required to provide a reason. The withdrawal mechanism must be:

- At least as simple, accessible, and prominent as the original consent mechanism;
- Available within the primary interface of the system — not buried in support documentation or accessible only through a customer service channel;
- Effective immediately upon user action — systems may not impose a "processing period" before withdrawal takes effect.

Upon withdrawal, collection of the relevant emotional data category must cease immediately. Data collected prior to withdrawal is subject to the retention schedule in Section 8 unless the user also exercises their Right of Deletion under Section 6.4.

6.2 Right of Access

Users may request a **complete record of all emotional data held about them**, including: the tier classification of each data element; the purpose for which it was collected; the date of collection; the retention schedule applicable to it; and any third parties with whom it has been shared. Access requests must be fulfilled within the timelines specified in Section 6.6.

6.3 Right of Correction

Users may request **correction of inaccurate emotional data** held about them. For inferred emotional data (Tier B), correction includes the right to dispute an inference and have it flagged or removed from the system's model of the user. Systems must document all correction requests and their resolution.

6.4 Right of Deletion

Users may request **deletion of all emotional data** held about them. Upon receipt of a valid deletion request, systems must:

11. Delete all Tier A and Tier B emotional data within 30 days;
12. Remove the user's individual data from Tier C aggregate datasets where technically feasible;
13. Instruct all third-party processors to delete the user's emotional data within the same timeframe;
14. Provide written confirmation of deletion upon request.

Limited exceptions apply where retention is required by applicable law. In such cases, the system must notify the user of the legal basis for retention and the expected retention period, and must restrict processing of the retained data to the minimum necessary to satisfy the legal obligation.

6.5 Right of Portability

Users may request their emotional data in a **portable, machine-readable format** (such as JSON or CSV). The exported data must include all Tier A and Tier B data elements, their tier classification, collection dates, and the purpose for which they were collected. Portability requests must be fulfilled within the timelines specified in Section 6.6.

6.6 Response Timelines

Right	Maximum Response Time	Extension Permitted
Access	30 calendar days from receipt of verified request	Yes — up to 30 additional days with written notice to user
Correction	30 calendar days from receipt of verified request	Yes — up to 30 additional days with written notice to user
Deletion	30 calendar days from receipt of verified request	No extension permitted
Portability	30 calendar days from receipt of verified request	Yes — up to 15 additional days with written notice to user
Withdrawal	Immediate upon user action	No extension permitted

Systems must provide users with a clearly documented process for submitting rights requests, including a designated contact, a confirmation of receipt within 5 business days, and a status update if the initial response deadline will not be met.

7. Data Minimization Requirements

Data minimization is a structural discipline, not an aspiration. EDCPS requires that emotional data collection be actively constrained — not merely limited in theory but demonstrably limited in practice — to what is genuinely necessary for each disclosed and consented purpose.

7.1 The Three-Part Minimization Test

Every category of emotional data collected by a subject system must satisfy all three of the following requirements:

- 15. Necessity:** The data is necessary for a purpose that has been specifically disclosed to the user in the consent instrument, and the system could not achieve that purpose without collecting data of that type. A general claim that more data improves model quality does not satisfy the necessity test.

16. **Proportionality:** The volume and sensitivity of the data collected is proportionate to the benefit the user receives from the service. Systems may not collect high-sensitivity emotional data to deliver low-value personalization features.
17. **Tier Minimization:** Systems must use the **lowest sensitivity tier sufficient** to accomplish the stated purpose. If a service purpose can be fulfilled using anonymized Tier C aggregate data, Tier A or Tier B individual data may not be used for that purpose.

7.2 Minimization Documentation

Systems must document minimization decisions for each category of emotional data collected. This documentation — referred to as the **Minimization Record** — must include:

Minimization Record Element	Required Content
Data Category	Specific description of the emotional data category
Tier Classification	Assigned tier under Section 3 and rationale for that classification
Disclosed Purpose	The specific service purpose for which collection is justified
Necessity Analysis	Explanation of why collection is necessary to achieve that purpose
Tier Justification	Explanation of why a lower-sensitivity tier is insufficient for the purpose
Proportionality Assessment	Assessment of service benefit delivered relative to sensitivity of data collected
Review Date	Date of most recent minimization review — must occur at least annually

Minimization Records must be made available to the CMOS-SB Standards Committee upon audit request. Systems that cannot produce current Minimization Records for all emotional data categories they collect are in non-compliance with this section regardless of their practices on the ground.

7.3 Feature and Service Design Obligations

Data minimization obligations attach at the design stage, not only at the point of implementation. Systems must incorporate minimization review into feature development processes so that emotional data collection requirements are assessed for necessity, proportionality, and tier efficiency before features are built, not after. Compliance-by-design is the expected standard under EDCPS.

DESIGN-STAGE OBLIGATION

Systems may not resolve minimization violations by simply adding a consent disclosure that covers unnecessary data collection. If the collection itself fails the three-part minimization test, the collection must be discontinued or redesigned — not papered over with consent language.

8. Retention and Deletion Standards

Emotional data must not be retained beyond the period necessary for the purpose for which it was collected. Retention is not a passive state — it is an active processing activity that must be continuously justified and technically enforced. EDCPS establishes maximum default retention periods for each tier and requires automated enforcement of those limits.

8.1 Maximum Retention Periods by Tier

Tier	Default Maximum Retention	Extension Conditions	Absolute Maximum
Tier A Direct Emotional Signals	90 days from date of collection	Extendable only with fresh, specific consent for a defined additional period and for a documented continuing purpose	365 days — no further extension permitted regardless of consent
Tier B Inferred Emotional States	180 days from date of collection	Extendable only with fresh, specific consent for a defined additional period and for a documented continuing purpose	730 days — no further extension permitted regardless of consent
Tier C Aggregate Emotional Indicators	365 days from date of aggregation	Extendable without individual consent where the data has been demonstrably anonymized and re-identification is not technically feasible	No absolute maximum — subject to periodic review and re-anonymization verification

The retention clock begins at the moment of collection (Tier A and Tier B) or the moment of aggregation (Tier C). Systems that refresh the retention clock by re-processing, re-modeling, or re-exporting previously collected data without a new collection event are in violation of this section.

8.2 Automated Deletion Workflows

Systems must implement **automated deletion workflows** that enforce retention limits without requiring any user action. Deletion may not be made contingent on the user submitting a deletion request — it must occur automatically when the retention period expires. Automated deletion workflows must:

18. Operate on a schedule that ensures deletion occurs within 7 days of the retention period expiry date;
19. Apply to all storage locations where emotional data is held, including backups, logs, and derived models that encode individual-level emotional data;
20. Generate an auditable deletion log that records the category, tier, retention period, and deletion date for each data element deleted;
21. Be tested no less than semi-annually to verify that deletion is occurring as designed.

8.3 Deletion Verification

Systems must provide users with **written confirmation of deletion** upon request, within 15 days of the deletion event. Confirmation must specify the categories of emotional data deleted, the date of deletion, and whether any data was retained under a legal-hold exception and the basis for that exception.

8.4 Derived Model Obligations

Where emotional data has been used to train or parameterize a model, and that model encodes individual-level emotional information, the individual's right of deletion extends to the model. Systems must either: (a) retrain the model excluding the user's data upon receipt of a valid deletion request; or (b) implement technically verified filtering that prevents the model from generating outputs that reflect the deleted individual's emotional data. Systems must document which approach is applied and make that documentation available upon request.

9. Third-Party Sharing Restrictions

The sharing of emotional data with third parties represents one of the highest-risk points in the emotional data lifecycle, as it places data beyond the direct control of the collecting system and into environments whose practices may be unknown to the user. EDCPS establishes a default no-share position and permits sharing only within narrowly defined conditions.

9.1 Default No-Share Principle

Emotional data — of all tiers — **may not be shared with third parties** without separate, explicit, granular consent from the user. This consent must be distinct from the consent obtained for collection and must specify:

- The identity or category of the third-party recipient;
- The specific tier(s) and category(ies) of emotional data to be shared;
- The purpose for which the third party will use the data;
- The retention period the third party will apply;
- Whether the third party will further share the data, and if so, under what conditions.

Generic consent language that authorizes sharing with "partners," "affiliates," or "service providers" without the specificity required above does not constitute valid sharing consent under EDCPS.

9.2 Prohibited Recipients

Regardless of user consent, emotional data may not be shared with the following categories of recipient for the following purposes:

Recipient Category	Prohibited Purpose	Scope of Prohibition
Advertisers and Ad Networks	Behavioral targeting, audience segmentation, or retargeting based on emotional state	All tiers — absolute prohibition

Recipient Category	Prohibited Purpose	Scope of Prohibition
Data Brokers	Any purpose — data brokers are defined as entities whose primary business is the aggregation and sale of personal data	All tiers — absolute prohibition
Law Enforcement	Sharing without valid legal process (court order, warrant, or equivalent)	All tiers — voluntary sharing prohibited; compelled sharing requires legal review and user notification where legally permissible
Political Organizations	Influencing political behavior, electoral participation, or political opinion without explicit, granular, and fully informed user consent	All tiers — requires the highest standard of consent disclosure
Commercial Entities	Influencing purchasing decisions or brand preferences without explicit, granular, and fully informed user consent	Tier A and Tier B — absolute prohibition without qualifying consent

9.3 Processor Agreements

Where emotional data is shared with third-party **processors** — entities that process emotional data on behalf of the collecting system rather than for their own purposes — such processors must be bound by written agreements that:

22. Impose EDCPS-equivalent data protection obligations on the processor;
23. Prohibit the processor from using emotional data for any purpose beyond those specified in the agreement;
24. Require the processor to implement equivalent automated deletion workflows;
25. Grant the collecting system the right to audit the processor's compliance;
26. Require the processor to notify the collecting system of any actual or suspected data breach within 48 hours;
27. Impose sub-processing restrictions equivalent to these requirements on any further delegation.

10. Special Population Protections

Certain populations require protections beyond the baseline EDCPS standards by virtue of their heightened vulnerability to the harms that emotional data misuse can produce, their reduced capacity to provide fully informed and autonomous consent, or the particular sensitivity of the contexts in which their emotional data arises. Enhanced protections under this section operate as a floor, not a ceiling — systems are encouraged to exceed them.

10.1 Minors

No emotional data of any tier may be collected from users who are under the age of majority in their jurisdiction without **verified parental or guardian consent**. Systems must implement age-verification processes proportionate to the risk of the emotional data collected. Assent from the minor user does not substitute for parental consent but may be obtained in addition to it for transparency purposes.

Additional obligations for minor users include:

- No behavioral profiling of minors based on emotional data for commercial purposes;
- Maximum retention of 30 days for Tier A data from minor users, regardless of parental consent to longer retention;
- Enhanced minimization obligations — only data strictly necessary for the specific service may be collected;
- No third-party sharing of minor users' emotional data for any commercial purpose, even with parental consent.

10.2 Users in Crisis States

Users in crisis states — defined as users who are exhibiting signals consistent with acute psychological distress, suicidal ideation, self-harm risk, or mental health crisis — are in a state of acutely elevated vulnerability in which meaningful autonomous consent is not reliably available. Accordingly:

- No emotional data collection during crisis interactions is permitted except where such collection is strictly necessary for the purpose of providing safety-relevant support;
- Data collected in the course of a crisis interaction must be classified as Tier A regardless of its technical derivation;

- Crisis-context emotional data must not be used for any purpose other than immediate safety response — no modeling, profiling, or commercial use;
- Crisis-context emotional data must be deleted within 90 days of the crisis interaction unless applicable law requires longer retention for safety review purposes.

10.3 Users in Healthcare Contexts

Emotional data collected in the context of healthcare interactions — including mental health platforms, wellness applications, telehealth services, and clinical tools — is subject to **maximum protection standards** under EDCPS, regardless of its tier classification. All emotional data from healthcare contexts is treated as Tier A for consent, retention, and sharing purposes. Systems operating in healthcare contexts must also comply with all applicable healthcare privacy regulations in addition to EDCPS requirements.

10.4 Users Who Have Disclosed Vulnerability

Where a user has explicitly disclosed a condition, circumstance, or history that increases their vulnerability to emotional data misuse — including but not limited to: history of trauma, active mental health treatment, cognitive disability, addiction recovery, or domestic violence — enhanced consent and minimization obligations apply:

- Enhanced consent disclosures must be provided, including explicit description of safeguards in place to protect vulnerable users;
- Minimization obligations are heightened — no data may be collected beyond what is strictly necessary for user-facing service delivery;
- No inferred emotional data modeling may be applied to disclosed-vulnerability users without additional explicit consent specifically addressing the inference process;
- Access to the user's emotional data must be restricted to the minimum number of personnel necessary.

Population	Consent Standard	Retention Standard	Sharing Standard
Minors	Verified parental consent required	Tier A: 30-day max	No commercial sharing regardless of consent

Population	Consent Standard	Retention Standard	Sharing Standard
Crisis States	Collection restricted to safety necessity only	90-day max for crisis data	No sharing beyond immediate safety function
Healthcare Contexts	All data treated as Tier A	Tier A standard applies regardless of tier	No commercial sharing; healthcare law applies
Disclosed Vulnerability	Enhanced consent required; inference requires additional consent	Strict minimization; shorter schedules preferred	Access and sharing restricted to service necessity

11. Prohibited Practices

The following practices are **absolutely prohibited** under EDCPS, regardless of user consent, contractual arrangement, technical necessity claim, or jurisdictional variation. No consent instrument, user agreement, or commercial relationship can authorize these practices. Systems found to have engaged in prohibited practices are subject to immediate compliance suspension pending remediation.

#	Prohibited Practice	Scope and Clarification
11.1	Emotional Manipulation	Using emotional data to influence users in ways that contradict their own stated interests, undermine their autonomous decision-making, or exploit identified vulnerabilities in their cognitive mode. This prohibition applies regardless of whether the manipulation is intended to benefit the user according to the system's assessment.
11.2	Context Transfer Without Consent	Using emotional data collected in one context (e.g., a wellness check-in) for a materially different purpose in a different context (e.g., commercial targeting) without fresh, specific, and fully informed consent for the new context and purpose.
11.3	Retention Beyond Permitted Periods	Retaining emotional data beyond the maximum retention periods established in Section 8, regardless of the reason. This includes retention in backup systems, log files, derived models, or third-party processor environments.

#	Prohibited Practice	Scope and Clarification
11.4	Sale of Emotional Data	Selling, licensing, or otherwise exchanging for commercial consideration any emotional data of any tier, in any form, whether individual-level or aggregated. The prohibition on sale applies even where the buyer claims to have independently derived the same data.
11.5	Discriminatory Use	Using emotional data to discriminate against users in the provision of services, pricing of products, prioritization of support, or any other service delivery dimension — regardless of whether the emotional state that is the basis of discrimination was voluntarily disclosed or inferred.
11.6	Re-identification of Aggregate Data	Aggregating, combining, cross-referencing, or otherwise processing Tier C emotional data in ways that result in or risk the re-identification of individual users. Systems must assess re-identification risk whenever new data sources are combined with Tier C data and must document the outcome of that assessment.
11.7	Denial of Core Service for Consent Refusal	Denying, degrading, or materially limiting a core service feature as a consequence of a user's refusal to consent to emotional data collection, where the emotional data is not strictly necessary for that specific feature to function.
11.8	Covert Collection	Collecting emotional data through any mechanism that is not disclosed to the user in the consent instrument, including through embedded components, third-party scripts, or technical inference processes that are not described in plain language in the consent disclosure.
11.9	Inferred State as Factual Record	Treating inferred emotional states (Tier B) as factual records of how the user felt, rather than as probabilistic inferences, when communicating data to the user, sharing with third parties, or using as the basis for consequential decisions.

COMPLIANCE NOTE — NON-WAIVABILITY

The prohibited practices in Section 11 are not subject to user waiver. A user may not consent to manipulation, discriminatory use, or re-identification of their data. Any purported consent instrument that authorizes a prohibited practice is void as against EDCPS policy and may not be used as a defense in any compliance proceeding.

12. Compliance Checklist

The following checklist is provided as a self-assessment and audit tool. Completion of this checklist does not constitute formal EDCPS certification but should be used by systems to assess readiness for formal audit. Each item must be completed with documentary evidence available upon request. Items answered "No" or "In Progress" require a documented remediation plan with target completion date.

System Name: _____ **Audit Date:** _____
Completed by: _____

#	Compliance Requirement	Yes	No	In Progress	Notes / Evidence Reference
1	EISS Prerequisite: System holds current EISS certification (CMOS-SB Standard 1002) prior to asserting EDCPS compliance.	☐	☐	☐	
2	Consent Architecture: Layered, tier-level consent architecture has been implemented with separate consent decisions for Tier A, Tier B, and Tier C data and by purpose.	☐	☐	☐	
3	Emotional Data Inventory: A current Emotional Data Inventory exists, documents all emotional data categories collected, their tier classifications, and is reviewed at least annually.	☐	☐	☐	
4	Tier Classification Applied: All emotional data has been classified into Tier A, Tier B, or Tier C with documented rationale for each classification.	☐	☐	☐	
5	Informed Consent Language: Consent disclosures include all nine required disclosure elements (Section 5.1), are written in plain language, and have been reviewed and approved.	☐	☐	☐	
6	Void Consent Practices Eliminated: System interfaces have been audited and confirmed free of dark patterns, pre-checked boxes, bundled consent, and coercive consent mechanisms.	☐	☐	☐	
7	Consent Ledger Operational: A Consent Ledger is in place recording all consent decisions with timestamps,	☐	☐	☐	

#	Compliance Requirement	Yes	No	In Progress	Notes / Evidence Reference
	version references, and scope documentation, and is accessible for audit.				
8	Withdrawal Mechanism Operational: A consent withdrawal mechanism is available within the primary interface, is as simple as the consent process, and takes effect immediately upon user action.	☐	☐	☐	
9	User Rights Response Process: A documented process exists for receiving, confirming, and responding to access, correction, deletion, and portability requests within EDCPS timelines.	☐	☐	☐	
10	Data Minimization Policy Documented: Minimization Records exist for all emotional data categories, including necessity analysis, tier justification, and proportionality assessment.	☐	☐	☐	
11	Retention Schedules Implemented: Maximum retention periods (Tier A: 90 days; Tier B: 180 days; Tier C: 365 days) are documented and enforced for all emotional data categories.	☐	☐	☐	
12	Automated Deletion Active: Automated deletion workflows are operational, have been tested within the last six months, apply to all storage locations including backups and logs, and generate auditable deletion logs.	☐	☐	☐	
13	Third-Party Sharing Controls: Default no-share is implemented; granular sharing consent is obtained before any third-party sharing; sharing with prohibited recipient categories is blocked at the system level.	☐	☐	☐	
14	Processor Agreements Updated: All third-party processor agreements include EDCPS-equivalent obligations, audit rights, breach notification requirements, and sub-processing restrictions.	☐	☐	☐	
15	Special Population Protections Implemented: Enhanced protections for minors, crisis-state users, healthcare-context users, and disclosed-vulnerability users are implemented and documented.	☐	☐	☐	
16	Prohibited Practices Audit Completed: A formal audit of system practices against the Section 11 prohibited practices list has been completed within the past 12 months with no unresolved findings.	☐	☐	☐	

#	Compliance Requirement	Yes	No	In Progress	Notes / Evidence Reference
17	Re-Consent Process Active: A documented process exists for identifying material changes to data practices and triggering fresh consent collection before new practices commence.	☐	☐	☐	
18	Derived Model Obligations Addressed: A policy exists for handling deletion requests that implicate trained models, specifying whether retraining or filtering is applied and documenting the approach.	☐	☐	☐	

Checklist Summary:

Result	Count
Yes (Compliant)	
No (Non-Compliant)	
In Progress (Partial)	
Total Items	18

CERTIFICATION READINESS GUIDANCE

Systems with all 18 items marked **Yes** with supporting documentary evidence may submit for formal EDCPS certification review with the CMOS-SB Standards Committee. Systems with any items marked **No** must complete remediation before submission. Systems with items marked **In Progress** may submit a conditional application with a documented remediation timeline, at the Committee's discretion.

Completed by (print name): _____

Title / Role: _____

Signature: _____ **Date:** _____

CMOS-SB Standard 1004 — EDCPS v1.0 | Issued June 9, 2026 | Next Review: June 9, 2027

Authored by Isabelle Anne Thompson | Published by CMOS-SB Standards Committee

Cognitive Mode OS™ is a trademark of Isabelle Anne Thompson / Sugar Sands Publishing LLC. All rights reserved.

cmos-sb.org

CMOS-SB Standard 1004 — EDCPS v1.0 | June 9, 2026 | cmos-sb.org