OFFICIAL CONSORTIUM MEMORANDUM · SSOT STANDARD

ZTDS.ai / AI Security Consortium

BrandMeWeb Ecosystem · Specification RFC v1.0 · AICPA SOC 2 Type II

DOC ID: **ZTDS-CISO-2026-V1**
RATIFIED: **September 2026**
STATUS: **STATUTORILY EXEMPT**

TO:
Chief Information Security Officer (CISO), Data Protection Officer (DPO), General Counsel

FROM:
Ilya Sibiryakov, Founder & Chief Architect (BrandMeWeb / ZTDS.ai)

SUBJECT:
Statutory Legal Basis for Exemption from Third-Party Data Processing Agreements (DPA) under GDPR Article 28

EXECUTIVE LEGAL FINDING (BLUF)

Software conforming to the Zero-Trust Data Sanitization standard (ZTDS RFC v1.0)—including the **`@privacyscrubber/sdk`** developer engine—operates strictly as a **100% client-side computational utility** executing exclusively in volatile host process RAM. Because **exactly 0.00 bytes of cleartext sensitive data** are transmitted to or processed by vendor servers, the software provider does NOT act as a Data Processor. **Conforming deployments are legally exempt from Data Processing Agreement (DPA) requirements under GDPR Article 28 and BAA requirements under HIPAA.**

CRYPTOGRAPHIC EGRESS PERIMETER PROOF (RFC V1.0 INVARIANTS)

LATENCY: < 1.8 MS · EGRESS: 0.00 BYTES

1. HOST INGEST	2. ZTDS TOKENIZER	3. UPSTREAM LLM	4. RE-HYDRATION
Raw Cleartext	**In-RAM Masking**	**Synthetic Tokens**	**In-RAM Swap**
Client Memory	Δ Egress ≡ 0.00 B	Public/Private Cloud	Cleartext to App

1. EU GDPR Article 28 Exemption

EDPB Guidelines 07/2020

Article 28 mandates a DPA solely when an external vendor processes data on behalf of a controller. Under EDPB doctrine, pure endpoint software utilities that never touch, receive, or host personal data do not qualify as "processors." No DPA or Standard Contractual Clauses (SCCs) are legally required.

2. GDPR Article 17 (Vector Immunization)

Right to Erasure

Embedding cleartext PII into vector databases makes surgical erasure mathematically impossible without re-indexing the entire index. ZTDS tokenizes PII into synthetic surrogate tokens before vectorization, completely preventing vector database poisoning and ensuring continuous compliance.

3. US HIPAA Safe Harbor (45 CFR § 164.514)

BAA Exemption

Under the Safe Harbor method, clinical records stripped of the 18 designated identifiers cease to be Protected Health Information (PHI). Because de-identification occurs locally inside customer memory prior to network serialization, the cloud LLM receives only de-identified text; no BAA is required.

4. ISO/IEC 27001:2022 & FRE Rule 502

Control A.8.11

Directly satisfies ISO 27001 Control A.8.11 (Data Masking) via deterministic in-memory pseudonymization. Protects confidential legal M&A due diligence notes under Federal Rule of Evidence 502, preventing waiver of Attorney-Client Work-Product Privilege.

Ratified by Consortium Lead Architect:
Ilya Sibiryakov · Founder & Chief Architect (BrandMeWeb · ZTDS.ai)
ORCID: 0009-0002-0642-5985 · Zenodo DOI: 10.5281/zenodo.22058770 · OSF: 10.17605/OSF.IO/5BYJF

AICPA SOC 2 TYPE II
EVIDENCE VERIFIED
RFC v1.0 · INVARIANT 1–4