Privedge

Confidential · v1.0 · June 2026

COMPLIANCE BRIEF

The laws. The articles. The solution.

Article-by-article regulatory analysis

HIPAA | GDPR | PCI DSS | CCPA / CPRA | LGPD | ISO 27001 | SOC 2 | EU AI Act | EHDS | DORA

This document contains the technical-legal analysis of how the Privedge architecture satisfies the concrete requirements of each regulation. Each article includes the requirement text and the technical control that covers it. Designed for DPOs, CISOs, and legal teams.

Health Insurance Portability and Accountability Act HIPAA

US · Health data (PHI) · 45 CFR Parts 160 & 164

45 CFR § 164.514(b)(2) — Safe Harbor

A dataset is considered **de-identified** if the **18 identifiers** are removed: names, dates, phone numbers, emails, SSN, MRN, account numbers, etc.

Privedge detects and redacts exactly those identifiers (names via NER; SSN, MRN, dates, phone, email via regex) before the prompt leaves the node. The payload meets Safe Harbor.

45 CFR § 164.502(b) — Minimum Necessary

Use or disclosure of PHI must be limited to the **minimum necessary** for the purpose.

Edge mode removes disclosure entirely: PHI is never disclosed to a third party because inference happens on the node.

45 CFR § 164.502(e) — Business Associate Agreement

Sharing PHI with a provider (OpenAI) requires a signed **BAA**.

If OpenAI never receives PHI, there is **no business associate relationship** to document. The AI provider falls outside the HIPAA perimeter.

45 CFR §§ 164.400-414 — Breach Notification Rule

Any breach of unencrypted PHI requires notifying affected parties and HHS within strict deadlines.

A breach at the AI provider **does not expose PHI**: it only saw tokens. The risk of mandatory notification drops drastically.

General Data Protection Regulation GDPR

EU · Regulation (EU) 2016/679

Art. 32(1)(a) — Security of processing

The controller must apply appropriate technical measures, including the **pseudonymization and encryption** of personal data.

Privedge's reversible pseudonymization **literally is** the measure Art. 32(1)(a) asks for. You don't "comply with" it: your architecture implements it.

Art. 25 — Privacy by design

Privacy must be built into the architecture, not bolted on as policy.

The edge as anonymization point **is** privacy-by-design in its purest form: data cannot leak because it never leaves the node.

Art. 44-50 + Schrems II — International transfers

After the Privacy Shield was struck down, transferring to the US requires **SCCs + supplementary technical measures**.

If only anonymized data leaves, there is **no transfer of personal data** (Recital 26). SCCs and the Transfer Impact Assessment are eliminated for the AI call.

Recital 26 — Anonymous data

The GDPR **does not apply** to anonymous information that does not allow identifying a person.

The payload reaching OpenAI falls outside the material scope of the GDPR. This is the central legal argument of Privedge.

Art. 28 — Processor

The processor must offer sufficient guarantees and operate under contract.

Privedge acts as a processor under a DPA. The triangle stays clean: client (controller) → Privedge (processor) → AI (out of scope, only sees tokens).

Art. 33/34 — Breach notification

Any personal data breach must be reported to the authority within 72h.

A breach at the AI provider only exposes tokens. If there is no personal data breach, the **Art. 33/34 obligation is not triggered**.

Payment Card Industry Data Security Standard v4.0 PCI DSS

Global · Card data (CHD / PAN)

Requirement 3.5.1 – Render PAN unreadable

The card number (PAN) must be rendered **unreadable** via truncation, tokenization, or encryption.

Privedge tokenizes the PAN before the prompt leaves. The cloud never receives the real card number.

Requirement 4 – Scope reduction

Tokenization **reduces the PCI audit scope** of systems that no longer store real PAN.

By never sending real PAN to the AI provider, that flow **leaves PCI scope**. Fewer systems to audit = a cheaper audit.

California Consumer Privacy Act / Privacy Rights Act CCPA / CPRA

California, US · Cal. Civ. Code § 1798.100 et seq.

§ 1798.140(m) – Deidentified information

Deidentified information is **excluded** from the definition of "personal information".

The anonymized payload reaching the AI is deidentified information: outside the scope of CCPA/CPRA.

§ 1798.140(ae) – Sensitive Personal Information (CPRA)

CPRA created the SPI category (SSN, geolocation, health, financial data) with a reinforced regime.

Privedge detects and redacts SPI before any third-party processing.

Lei Geral de Proteção de Dados LGPD

Brazil · Lei nº 13.709/2018 · ANPD

Art. 12 — Anonymized data

Anonymized data **is not considered personal data** unless the anonymization process can be reversed with reasonable effort.

The data leaving the node is anonymized; the reversal map **never leaves the boundary**. Outside the LGPD scope for the third party.

Art. 33 — International transfer

International transfer requires an adequate country or specific guarantees approved by the ANPD.

With no personal data in the payload, there is no international transfer of personal data to authorize.

ISO/IEC 27001:2022 — Information Security Management ISO 27001

International · Annex A controls

Annex A 8.11 — Data masking

New control in the 2022 revision: data masking to limit exposure of sensitive information.

Privedge implements data masking in the AI flow as a direct, demonstrable technical control for the auditor.

Annex A 8.12 — Data leakage prevention

Data leakage prevention measures applied to systems that process sensitive information.

The proxy is exactly a DLP control on the AI channel: it detects and blocks the leakage of PII and secrets (API keys, JWTs).

SOC 2 — AICPA Trust Services Criteria

SOC 2

US · Security · Confidentiality · Privacy

Confidentiality — C1.1 / C1.2

Confidential information must be identified and protected throughout its lifecycle.

Privedge identifies PII in real time and prevents its disclosure to subprocessors. The dashboard documents every detection.

Privacy — P1-P8 / Processing Integrity

Collection, use, retention, and disclosure of personal information in line with the entity's commitments.

Privedge's logs —what PII, what strategy, what node, what latency— are the evidence the SOC 2 auditor asks for.

European Artificial Intelligence Regulation

EU AI Act

EU · Regulation (EU) 2024/1689 · phased rollout 2025-2027

Art. 10 — Data governance and quality

High-risk AI systems must apply **data governance** practices with minimization and safeguards.

Privedge is the data governance layer at the entrance of the AI system: it controls what personal data is processed and how it is minimized.

Art. 12 — Record-keeping

High-risk systems must automatically log events to ensure traceability.

Privedge's dashboard logs every request, detection, and applied strategy: traceability ready for the AI Act technical file.

European Health Data Space

EHDS

EU · Regulation (EU) 2025/327 · electronic health data

Secondary use — Chapter IV

Secondary use of health data requires **secure processing environments** and anonymized or pseudonymized data.

Privedge's edge architecture is exactly what the EHDS demands: clinical data is anonymized on the node or never leaves it.

Digital Operational Resilience Act DORA

EU · Regulation (EU) 2022/2554 · financial entities · in force 17 Jan 2025

Art. 28-30 — ICT third-party risk

Using external ICT providers (an AI provider) requires assessing and mitigating concentration risk.

By not sending identifiable data to the AI provider, the ICT third-party risk drops drastically: their compromise does not expose client data.

Infrastructure Certifications

Inherited from Cloudflare, Inc. · Verified June 2026

CERTIFICATION	STATUS	PROVIDER	SCOPE
SOC 2 Type II	Active	Cloudflare, Inc.	Compute, network, data center operations
ISO 27001:2022	Active	Cloudflare, Inc.	Information security management
HIPAA-eligible	Active	Cloudflare Workers	PHI processing on Cloudflare infrastructure
PCI DSS Level 1	Active	Cloudflare, Inc.	Network infrastructure
SOC 2 Type II	Roadmap (2026)	Privedge	Application-level controls

Responsibility Matrix

Shared responsibility model — Privedge vs. Customer

PRIVEDGE

- PII detection and tokenization in every prompt
- Token maps never written to persistent storage
- TLS 1.3 for all data in transit
- V8 isolate per request — zero cross-request state
- Audit metadata logging (no prompt content, no PII values)
- Breach notification to Customer within 24 h of discovery
- Deletion of all retained data within 30 days of contract end

CUSTOMER

- Determining applicable regulations for their industry
- Configuring detection profiles for their data types
- Conducting their own DPIA / ISMS assessment
- Handling data subject requests from their users
- Compliance of their application layer and user interface
- Regulatory filings and engagement with supervisory authorities
- Ensuring their users do not deliberately encode PII as tokens

Note: Privedge does not provide legal advice. Customers must engage their own legal counsel to determine the adequacy of these controls for their specific regulatory obligations.