

anonym.plus

T2 — IRREVERSIBILITY

10 Case Studies — Problem Analysis & Solution Architecture

SOLID — Directly addressable through technical measures

Generated: February 2026
Source: anonym.community
Product version: v8.3.1

Table of Contents

01 Biometric immutability

Evidence refs: 1.3, 4.6, 15.9

02 Backup persistence

Evidence refs: 3.3, 16.9

03 Third-party propagation

Evidence refs: 3.7

04 Shadow profiles

Evidence refs: 3.2

05 Git history

Evidence refs: 16.1

06 ML model memorization

Evidence refs: 15.5, 16.2

07 De-indexing illusion

Evidence refs: 3.8

08 Breach databases

Evidence refs: 16.4

09 Cache/index/warehouse copies

Evidence refs: 16.9

10 Surveillance advertising records

Evidence refs: 1.10

Transistor: T2 — IRREVERSIBILITY

Definition: Once PII propagates, it cannot be un-propagated.

01. Biometric immutability

Evidence refs: 1.3, 4.6, 15.9

Executive Summary

Biometric immutability represents a critical privacy challenge: You cannot change your face, fingerprints, or DNA after a breach. This pain point is driven by IRREVERSIBILITY — once pii propagates, it cannot be un-propagated. anonym.plus addresses this through 100% local processing with AES-256-GCM encrypted vault — PII processed and stored locally, never touching any external server.

The Problem

You cannot change your face, fingerprints, or DNA after a breach. Compromised faceprints are permanent — unlike passwords, there is no reset

Root cause: T2 — IRREVERSIBILITY: Once PII propagates, it cannot be un-propagated.

The Solution: How anonym.plus Addresses This

Detection Capabilities

anonym.plus identifies 200+ entity types including biometric references, facial descriptions, fingerprint mentions, DNA identifiers. The local Presidio 2.2.357 + spaCy 3.8.11 architecture uses Presidio 2.2.357 deterministic recognizers with 121 built-in presets for structured identifiers and spaCy 3.8.11 with 23 language models, all running locally via FastAPI sidecar for contextual references.

Anonymization Methods

Redact is recommended: permanently removing biometric references ensures they cannot be compromised from document breaches — critical because biometric data cannot be reset. Encrypt provides an alternative — AES-256-GCM encryption enables authorized access while protecting at rest, providing the only reversible option for data that cannot be re-issued.

Architecture & Deployment

100% local processing — data never leaves the device. Presidio 2.2.357 sidecar runs all detection locally with spaCy 3.8.11 (23 models). After activation, fully offline operation.

Compliance Mapping

This pain point intersects with GDPR Article 9 special category biometric data, HIPAA protected health information. anonym.plus's GDPR (data never leaves device), HIPAA (local processing) compliance coverage, combined with 100% local — data never leaves device hosting, provides documented technical measures for regulatory submissions.

02. Backup persistence

Evidence refs: 3.3, 16.9

[Executive Summary](#)

Backup persistence represents a critical privacy challenge: Deleted from production but alive in nightly, weekly, monthly backups. This pain point is driven by IRREVERSIBILITY — once pii propagates, it cannot be un-propagated. anonym.plus addresses this through 100% local processing with AES-256-GCM encrypted vault — PII processed and stored locally, never touching any external server.

[The Problem](#)

Deleted from production but alive in nightly, weekly, monthly backups. Redis cache, Elasticsearch, Kafka topics, Snowflake all retain after 'deletion'

Root cause: T2 — IRREVERSIBILITY: Once PII propagates, it cannot be un-propagated.

[The Solution: How anonym.plus Addresses This](#)

[Detection Capabilities](#)

anonym.plus identifies 200+ entity types including personally identifiable records, database field names, system identifiers. The local Presidio 2.2.357 + spaCy 3.8.11 architecture uses Presidio 2.2.357 deterministic recognizers with 121 built-in presets for structured identifiers and spaCy 3.8.11 with 23 language models, all running locally via FastAPI sidecar for contextual references.

[Anonymization Methods](#)

Redact is recommended: anonymizing data before it enters any storage system prevents the backup persistence problem at its source. Replace provides an alternative — substituting PII with anonymized alternatives before storage ensures backups contain no personal data. For reversibility, Encrypt (AES-256-GCM) enables authorized recovery.

[Architecture & Deployment](#)

Zero cloud dependency after activation. Ed25519 machine-bound licensing requires only initial activation — subsequent operations are completely offline. All processing stays local.

[Compliance Mapping](#)

This pain point intersects with GDPR Article 17 right to erasure, Article 5(1)(e) storage limitation. anonym.plus's GDPR (data never leaves device), HIPAA (local processing) compliance coverage, combined with 100% local — data never leaves device hosting, provides documented technical measures for regulatory submissions.

03. Third-party propagation

Evidence refs: 3.7

[Executive Summary](#)

Third-party propagation represents a critical privacy challenge: PII broadcast via RTB to thousands of unknown companies cannot be recalled. This pain point is driven by IRREVERSIBILITY — once pii propagates, it cannot be un-propagated. anonym.plus addresses this through 100% local processing with AES-256-GCM encrypted vault — PII processed and stored locally, never touching any external server.

[The Problem](#)

PII broadcast via RTB to thousands of unknown companies cannot be recalled. No mechanism to verify downstream deletion

Root cause: T2 — IRREVERSIBILITY: Once PII propagates, it cannot be un-propagated.

[The Solution: How anonym.plus Addresses This](#)

[Detection Capabilities](#)

anonym.plus identifies 200+ entity types including names, email addresses, advertising IDs, device identifiers, behavioral profiles. The local Presidio 2.2.357 + spaCy 3.8.11 architecture uses Presidio 2.2.357 deterministic recognizers with 121 built-in presets for structured identifiers and spaCy 3.8.11 with 23 language models, all running locally via FastAPI sidecar for contextual references.

[Anonymization Methods](#)

Redact is recommended: anonymizing PII before sharing with third parties prevents propagation that makes recall impossible. Replace provides an alternative — substituting identifiers before third-party sharing maintains data utility while preventing individual tracking. For reversibility, Encrypt (AES-256-GCM) enables authorized recovery.

[Architecture & Deployment](#)

The local sidecar REST API (port 5002-5003) provides programmatic access to Presidio detection for local development workflow integration.

[Compliance Mapping](#)

This pain point intersects with GDPR Article 28 processor obligations, Article 44 transfer restrictions. anonym.plus's GDPR (data never leaves device), HIPAA (local processing) compliance coverage, combined with 100% local — data never leaves device hosting, provides documented technical measures for regulatory submissions.

04. Shadow profiles

Evidence refs: 3.2

[Executive Summary](#)

Shadow profiles represents a critical privacy challenge: Facebook maintains profiles of non-users from contact uploads, Pixel browsing data, and Like button interactions. This pain point is driven by IRREVERSIBILITY — once pii propagates, it cannot be un-propagated. anonym.plus addresses this through 100% local processing with AES-256-GCM encrypted vault — PII processed and stored locally, never touching any external server.

[The Problem](#)

Facebook maintains profiles of non-users from contact uploads, Pixel browsing data, and Like button interactions. PII about you that you never provided

Root cause: T2 — IRREVERSIBILITY: Once PII propagates, it cannot be un-propagated.

[The Solution: How anonym.plus Addresses This](#)

[Detection Capabilities](#)

anonym.plus identifies 200+ entity types including names, email addresses, phone numbers, contact information, browsing identifiers. The local Presidio 2.2.357 + spaCy 3.8.11 architecture uses Presidio 2.2.357 deterministic recognizers with 121 built-in presets for structured identifiers and spaCy 3.8.11 with 23 language models, all running locally via FastAPI sidecar for contextual references.

[Anonymization Methods](#)

Redact is recommended: removing identifying information prevents creation of shadow profiles by ensuring no third-party PII is included in shared data. Replace provides an alternative — replacing contact details with placeholders preserves document structure while protecting non-users. For reversibility, Encrypt (AES-256-GCM) enables authorized recovery.

[Architecture & Deployment](#)

The Tauri 2.x desktop application (Rust + React) processes 7 document formats (PDF, DOCX, XLSX, TXT, CSV, JSON, XML) plus images (Tesseract OCR). AES-256-GCM vault with Argon2id protects all stored data.

[Compliance Mapping](#)

This pain point intersects with GDPR Article 14 information for data subjects not directly collected from, Article 6 lawful basis. anonym.plus's GDPR (data never leaves device), HIPAA (local processing) compliance coverage, combined with 100% local — data never leaves device hosting, provides documented technical measures for regulatory submissions.

05. Git history

Evidence refs: 16.1

[Executive Summary](#)

Git history represents a critical privacy challenge: Committed secrets persist in version control permanently. This pain point is driven by IRREVERSIBILITY — once pii propagates, it cannot be un-propagated. anonym.plus addresses this through 100% local processing with AES-256-GCM encrypted vault — PII processed and stored locally, never touching any external server.

[The Problem](#)

Committed secrets persist in version control permanently. Bots detect exposed credentials within minutes. BFG Repo-Cleaner can't undo what was already scraped

Root cause: T2 — IRREVERSIBILITY: Once PII propagates, it cannot be un-propagated.

[The Solution: How anonym.plus Addresses This](#)

[Detection Capabilities](#)

anonym.plus identifies 200+ entity types including API keys, access tokens, passwords, database credentials, private keys. The local Presidio 2.2.357 + spaCy 3.8.11 architecture uses Presidio 2.2.357 deterministic recognizers with 121 built-in presets for structured identifiers and spaCy 3.8.11 with 23 language models, all running locally via FastAPI sidecar for contextual references.

[Anonymization Methods](#)

Redact is recommended: removing credentials from code and documents before version control eliminates the exposure vector. Replace provides an alternative — substituting credentials with placeholder tokens maintains documentation while removing actual secrets. For reversibility, Encrypt (AES-256-GCM) enables authorized recovery.

[Architecture & Deployment](#)

While anonym.plus does not include MCP integration, its local sidecar API (port 5002-5003) provides REST endpoints for text analysis, image analysis, and model management.

[Compliance Mapping](#)

This pain point intersects with GDPR Article 32 security of processing, ISO 27001 access control. anonym.plus's GDPR (data never leaves device), HIPAA (local processing) compliance coverage, combined with 100% local — data never leaves device hosting, provides documented technical measures for regulatory submissions.

06. ML model memorization

Evidence refs: 15.5, 16.2

Executive Summary

ML model memorization represents a critical privacy challenge: GPT-style models memorize and reproduce training data — phone numbers, emails, PII baked into model weights that cannot be extracted or deleted. This pain point is driven by IRREVERSIBILITY — once pii propagates, it cannot be un-propagated. anonym.plus addresses this through 100% local processing with AES-256-GCM encrypted vault — PII processed and stored locally, never touching any external server.

The Problem

GPT-style models memorize and reproduce training data — phone numbers, emails, PII baked into model weights that cannot be extracted or deleted

Root cause: T2 — IRREVERSIBILITY: Once PII propagates, it cannot be un-propagated.

The Solution: How anonym.plus Addresses This

Detection Capabilities

anonym.plus identifies 200+ entity types including names, emails, phone numbers, medical records, training data with PII. The local Presidio 2.2.357 + spaCy 3.8.11 architecture uses Presidio 2.2.357 deterministic recognizers with 121 built-in presets for structured identifiers and spaCy 3.8.11 with 23 language models, all running locally via FastAPI sidecar for contextual references.

Anonymization Methods

Replace is recommended: substituting PII in training data with realistic synthetic alternatives preserves statistical properties while preventing memorization. Redact provides an alternative — removing PII entirely from training data eliminates memorization risk at the cost of reduced training diversity. For reversibility, Encrypt (AES-256-GCM) enables authorized recovery.

Architecture & Deployment

Documents and datasets are batch-anonymized before ML training. The 200+ entity types with 121 presets cover common training data PII patterns. Processed data never leaves the machine.

Compliance Mapping

This pain point intersects with GDPR Article 25 data protection by design, Article 5(1)(c) minimization. anonym.plus's GDPR (data never leaves device), HIPAA (local processing) compliance coverage, combined with 100% local — data never leaves device hosting, provides documented technical measures for regulatory submissions.

07. De-indexing illusion

Evidence refs: 3.8

[Executive Summary](#)

De-indexing illusion represents a critical privacy challenge: Google removes search results but original page, cached copies, Wayback Machine copies remain. This pain point is driven by IRREVERSIBILITY — once pii propagates, it cannot be un-propagated. anonym.plus addresses this through 100% local processing with AES-256-GCM encrypted vault — PII processed and stored locally, never touching any external server.

[The Problem](#)

Google removes search results but original page, cached copies, Wayback Machine copies remain. Geographic limits: same search from outside EU returns full results

Root cause: T2 — IRREVERSIBILITY: Once PII propagates, it cannot be un-propagated.

[The Solution: How anonym.plus Addresses This](#)

[Detection Capabilities](#)

anonym.plus identifies 200+ entity types including names, addresses, contact details, identifying descriptions, biographical information. The local Presidio 2.2.357 + spaCy 3.8.11 architecture uses Presidio 2.2.357 deterministic recognizers with 121 built-in presets for structured identifiers and spaCy 3.8.11 with 23 language models, all running locally via FastAPI sidecar for contextual references.

[Anonymization Methods](#)

Redact is recommended: anonymizing documents at creation prevents PII from appearing in any cached, indexed, or archived copy. Replace provides an alternative — substituting identifiers before publication ensures cached copies contain only anonymized data. For reversibility, Encrypt (AES-256-GCM) enables authorized recovery.

[Architecture & Deployment](#)

The Tauri 2.x desktop application (Rust + React) processes 7 document formats (PDF, DOCX, XLSX, TXT, CSV, JSON, XML) plus images (Tesseract OCR). AES-256-GCM vault with Argon2id protects all stored data.

[Compliance Mapping](#)

This pain point intersects with GDPR Article 17 right to erasure, Article 17(2) obligation to inform recipients. anonym.plus's GDPR (data never leaves device), HIPAA (local processing) compliance coverage, combined with 100% local — data never leaves device hosting, provides documented technical measures for regulatory submissions.

08. Breach databases

Evidence refs: 16.4

[Executive Summary](#)

Breach databases represents a critical privacy challenge: Have I Been Pwned: 13B+ breached accounts. This pain point is driven by IRREVERSIBILITY — once pii propagates, it cannot be un-propagated. anonym.plus addresses this through 100% local processing with AES-256-GCM encrypted vault — PII processed and stored locally, never touching any external server.

[The Problem](#)

Have I Been Pwned: 13B+ breached accounts. Once PII appears in a breach database, it persists indefinitely across the internet

Root cause: T2 — IRREVERSIBILITY: Once PII propagates, it cannot be un-propagated.

[The Solution: How anonym.plus Addresses This](#)

[Detection Capabilities](#)

anonym.plus identifies 200+ entity types including email addresses, passwords, usernames, IP addresses, account identifiers. The local Presidio 2.2.357 + spaCy 3.8.11 architecture uses Presidio 2.2.357 deterministic recognizers with 121 built-in presets for structured identifiers and spaCy 3.8.11 with 23 language models, all running locally via FastAPI sidecar for contextual references.

[Anonymization Methods](#)

Encrypt is recommended: AES-256-GCM encryption of credentials in documents enables authorized access for incident response while protecting at rest. Hash provides an alternative — SHA-256 hashing enables breach impact analysis without exposing original values.

[Architecture & Deployment](#)

Zero cloud dependency after activation. Ed25519 machine-bound licensing requires only initial activation — subsequent operations are completely offline. All processing stays local.

[Compliance Mapping](#)

This pain point intersects with GDPR Articles 33-34 breach notification, Article 32 security measures. anonym.plus's GDPR (data never leaves device), HIPAA (local processing) compliance coverage, combined with 100% local — data never leaves device hosting, provides documented technical measures for regulatory submissions.

09. Cache/index/warehouse copies

Evidence refs: 16.9

[Executive Summary](#)

Cache/index/warehouse copies represents a critical privacy challenge: After 'deletion': data in nightly backups, Redis, Elasticsearch, Kafka, Sentry, Amplitude, Mailchimp. This pain point is driven by IRREVERSIBILITY — once pii propagates, it cannot be un-propagated. anonym.plus addresses this through 100% local processing with AES-256-GCM encrypted vault — PII processed and stored locally, never touching any external server.

[The Problem](#)

After 'deletion': data in nightly backups, Redis, Elasticsearch, Kafka, Sentry, Amplitude, Mailchimp. Dozens of copies across dozens of systems

Root cause: T2 — IRREVERSIBILITY: Once PII propagates, it cannot be un-propagated.

[The Solution: How anonym.plus Addresses This](#)

[Detection Capabilities](#)

anonym.plus identifies 200+ entity types including user records, analytics data, behavioral logs, transaction records. The local Presidio 2.2.357 + spaCy 3.8.11 architecture uses Presidio 2.2.357 deterministic recognizers with 121 built-in presets for structured identifiers and spaCy 3.8.11 with 23 language models, all running locally via FastAPI sidecar for contextual references.

[Anonymization Methods](#)

Redact is recommended: anonymizing data before it enters caching systems eliminates the dozens-of-copies problem. Replace provides an alternative — substituting identifiers before downstream systems enables analytics without PII copies in Redis, Elasticsearch, Kafka. For reversibility, Encrypt (AES-256-GCM) enables authorized recovery.

[Architecture & Deployment](#)

Zero cloud dependency after activation. Ed25519 machine-bound licensing requires only initial activation — subsequent operations are completely offline. All processing stays local.

[Compliance Mapping](#)

This pain point intersects with GDPR Article 5(1)(e) storage limitation, Article 25 data protection by design. anonym.plus's GDPR (data never leaves device), HIPAA (local processing) compliance coverage, combined with 100% local — data never leaves device hosting, provides documented technical measures for regulatory submissions.

10. Surveillance advertising records

Evidence refs: 1.10

[Executive Summary](#)

Surveillance advertising records represents a critical privacy challenge: RTB bid streams processed 100B+ times daily. This pain point is driven by IRREVERSIBILITY — once pii propagates, it cannot be un-propagated. anonym.plus addresses this through 100% local processing with AES-256-GCM encrypted vault — PII processed and stored locally, never touching any external server.

[The Problem](#)

RTB bid streams processed 100B+ times daily. Records persist across ad exchanges, DSPs, DMPs. No recall mechanism exists

Root cause: T2 — IRREVERSIBILITY: Once PII propagates, it cannot be un-propagated.

[The Solution: How anonym.plus Addresses This](#)

[Detection Capabilities](#)

anonym.plus identifies 200+ entity types including advertising IDs, browsing history, location data, interest profiles, bid parameters. The local Presidio 2.2.357 + spaCy 3.8.11 architecture uses Presidio 2.2.357 deterministic recognizers with 121 built-in presets for structured identifiers and spaCy 3.8.11 with 23 language models, all running locally via FastAPI sidecar for contextual references.

[Anonymization Methods](#)

Redact is recommended: removing identifiers before data enters advertising systems prevents permanent surveillance records. Replace provides an alternative — substituting advertising identifiers with non-trackable alternatives enables aggregate analytics without surveillance. For reversibility, Encrypt (AES-256-GCM) enables authorized recovery.

[Architecture & Deployment](#)

The local sidecar REST API (port 5002-5003) provides programmatic access to Presidio detection for local development workflow integration.

[Compliance Mapping](#)

This pain point intersects with GDPR Article 6 lawful basis, ePrivacy consent requirements, Article 21 right to object. anonym.plus's GDPR (data never leaves device), HIPAA (local processing) compliance coverage, combined with 100% local — data never leaves device hosting, provides documented technical measures for regulatory submissions.

Product Specifications

App Version v8.3.1

Entity Types 200+ built-in, up to 50 custom

Detection Engine Presidio 2.2.357 + spaCy 3.8.11 (23 models)

Languages 48 UI, 23 NLP models

Document Formats PDF, DOCX, XLSX, TXT, CSV, JSON, XML + Image OCR

Anonymization Methods Replace, Redact, Mask, Hash (SHA-256/512/MD5), Encrypt (AES-256-GCM)

Architecture Tauri 2.x (Rust + React) + FastAPI sidecar (~370 MB)

Licensing Ed25519 signed, machine-fingerprinted, max 5 machines

Processing 100% local — data never leaves device

Compliance GDPR, HIPAA (data residency guaranteed by local processing)

Other Products Addressing This Transistor

- cloak.business (Air-gapped desktop)

Online versions available at:

<https://anonym.community/anonym.plus/>

© 2026 curta.solutions & anonym.plus. All rights reserved.

