anonymize.solutions

T7 — JURISDICTION FRAGMENTATION

10 Case Studies — Problem Analysis & Solution Architecture

STRUCTURAL LIMIT — Dashed transistor: fundamental dynamic that no technology can fully resolve

Generated: February 2026
Source: anonym.community
Product version: v1.6.12

Table of Contents

Transistor: T7 — JURISDICTION FRAGMENTATION
Definition: PII flows globally in milliseconds.

T7 JURISDICTION FRAGMENTATION — Case Study 1 of 10

01. US federal law absence

Evidence refs: 1.1

Executive Summary

US federal law absence represents a critical privacy challenge: No comprehensive federal privacy law in the world's largest tech economy. This pain point is driven by JURISDICTION FRAGMENTATION — pii flows globally in milliseconds. anonymize.solutions addresses this through 100% EU hosting (Hetzner Germany, ISO 27001) with Self-Managed Docker deployment enabling data localization in any jurisdiction.

The Problem

No comprehensive federal privacy law in the world's largest tech economy. Patchwork of HIPAA, FERPA, COPPA, and 50 state laws. Data brokers operate in regulatory void

Root cause: T7 — JURISDICTION FRAGMENTATION: PII flows globally in milliseconds.

The Solution: How anonymize.solutions Addresses This

Detection Capabilities

anonymize.solutions identifies 260+ entity types including SSNs, state-specific identifiers, HIPAA records, FERPA data, financial accounts. The dual-layer (regex + NLP) architecture uses 210+ custom pattern recognizers (246 patterns, 75+ country formats, checksum-validated) for structured identifiers and spaCy (25 languages) + Stanza (7 languages) + XLM-RoBERTa (16 languages) for contextual references.

Anonymization Methods

Redact is recommended: anonymizing PII across all US regulatory categories using a single platform eliminates the patchwork compliance problem. Hash provides an alternative — SHA-256 hashing enables cross-system integrity while satisfying anonymization across HIPAA, FERPA, and state laws. For reversibility, Encrypt (AES-256-GCM) enables authorized recovery.

Architecture & Deployment

100% EU hosting (Hetzner Germany, ISO 27001) satisfies GDPR data residency. Self-Managed deployment (Docker) enables data localization in any jurisdiction. Compliance spans GDPR, HIPAA, FERPA, PCI-DSS, ISO 27001.

Structural Limits

This pain point stems from JURISDICTION FRAGMENTATION, a structural dynamic that no technology can fully resolve. Within these limits, anonymize.solutions provides targeted mitigations: No technology can create a US federal privacy law. The platform's multi-regulation compliance (GDPR, HIPAA, FERPA, PCI-DSS) enables organizations to meet requirements across the patchwork from a single deployment.

Compliance Mapping

This pain point intersects with HIPAA Privacy Rule, FERPA student records, COPPA, CCPA consumer rights. anonymize.solutions’s GDPR, HIPAA, FERPA, PCI-DSS, ISO 27001 compliance coverage, combined with 100% EU (Hetzner Germany, ISO 27001) hosting, provides documented technical measures for regulatory submissions.

T7 JURISDICTION FRAGMENTATION — Case Study 2 of 10

02. GDPR enforcement bottleneck

Evidence refs: 2.1

Executive Summary

GDPR enforcement bottleneck represents a critical privacy challenge: Ireland's DPC handles most Big Tech complaints. This pain point is driven by JURISDICTION FRAGMENTATION — pii flows globally in milliseconds. anonymize.solutions addresses this through 100% EU hosting (Hetzner Germany, ISO 27001) with Self-Managed Docker deployment enabling data localization in any jurisdiction.

The Problem

Ireland's DPC handles most Big Tech complaints. 3-5 year delays. noyb filed 100+ complaints — many still unresolved. Overruled by EDPB repeatedly

Root cause: T7 — JURISDICTION FRAGMENTATION: PII flows globally in milliseconds.

The Solution: How anonymize.solutions Addresses This

Detection Capabilities

anonymize.solutions identifies 260+ entity types including EU citizen data, cross-border transfer records, processing logs, consent records. The dual-layer (regex + NLP) architecture uses 210+ custom pattern recognizers (246 patterns, 75+ country formats, checksum-validated) for structured identifiers and spaCy (25 languages) + Stanza (7 languages) + XLM-RoBERTa (16 languages) for contextual references.

Anonymization Methods

Redact is recommended: anonymizing PII before it becomes subject to regulatory disputes eliminates the enforcement bottleneck — anonymized data is outside GDPR scope. Replace provides an alternative — substituting identifiers reduces regulatory surface area requiring multi-year DPC investigation. For reversibility, Encrypt (AES-256-GCM) enables authorized recovery.

Architecture & Deployment

100% EU hosting (Hetzner Germany, ISO 27001) satisfies GDPR data residency. Self-Managed deployment (Docker) enables data localization in any jurisdiction. Compliance spans GDPR, HIPAA, FERPA, PCI-DSS, ISO 27001.

Structural Limits

This pain point stems from JURISDICTION FRAGMENTATION, a structural dynamic that no technology can fully resolve. Within these limits, anonymize.solutions provides targeted mitigations: 3-5 year enforcement delays represent a structural bottleneck no technology resolves. Anonymizing data reduces the personal data subject to GDPR, reducing the regulatory surface area feeding the backlog.

Compliance Mapping

This pain point intersects with GDPR Articles 56-60 cross-border cooperation, Article 83 administrative fines. anonymize.solutions’s GDPR, HIPAA, FERPA, PCI-DSS, ISO 27001 compliance coverage, combined with 100% EU (Hetzner Germany, ISO 27001) hosting, provides documented technical measures for regulatory submissions.

03. Cross-border conflicts

Evidence refs: 1.8

Executive Summary

Cross-border conflicts represents a critical privacy challenge: GDPR demands protection vs CLOUD Act demands access vs China's NSL demands localization. This pain point is driven by JURISDICTION FRAGMENTATION — pii flows globally in milliseconds. anonymize.solutions addresses this through 100% EU hosting (Hetzner Germany, ISO 27001) with Self-Managed Docker deployment enabling data localization in any jurisdiction.

The Problem

GDPR demands protection vs CLOUD Act demands access vs China's NSL demands localization. Creates impossible simultaneous compliance

Root cause: T7 — JURISDICTION FRAGMENTATION: PII flows globally in milliseconds.

The Solution: How anonymize.solutions Addresses This

Detection Capabilities

anonymize.solutions identifies 260+ entity types including data subject records under multiple jurisdictions, CLOUD Act responsive data. The dual-layer (regex + NLP) architecture uses 210+ custom pattern recognizers (246 patterns, 75+ country formats, checksum-validated) for structured identifiers and spaCy (25 languages) + Stanza (7 languages) + XLM-RoBERTa (16 languages) for contextual references.

Anonymization Methods

Encrypt is recommended: AES-256-GCM encryption enables organizational control with jurisdictional flexibility — encrypted data protected from unauthorized government access. Redact provides an alternative — complete PII removal eliminates cross-border conflicts — anonymized data is not subject to GDPR, CLOUD Act, or NSL simultaneously.

Architecture & Deployment

Self-Managed deployment (Docker containers, air-gapped option) eliminates cloud dependency entirely. Managed Private provides dedicated EU infrastructure with customer-managed encryption keys.

Structural Limits

This pain point stems from JURISDICTION FRAGMENTATION, a structural dynamic that no technology can fully resolve. Within these limits, anonymize.solutions provides targeted mitigations: GDPR demands protection vs CLOUD Act demands access vs China demands localization. Self-Managed deployment (Docker) enables organizations to localize processing within each jurisdiction.

Compliance Mapping

This pain point intersects with GDPR Chapter V transfers, US CLOUD Act, China PIPL data localization. anonymize.solutions’s GDPR, HIPAA, FERPA, PCI-DSS, ISO 27001 compliance coverage, combined with 100% EU (Hetzner Germany, ISO 27001) hosting, provides documented technical measures for regulatory submissions.

T7 JURISDICTION FRAGMENTATION — Case Study 4 of 10

04. Global South law absence

Evidence refs: 7.3

Executive Summary

Global South law absence represents a critical privacy challenge: Only ~35 of 54 African countries have data protection laws. This pain point is driven by JURISDICTION FRAGMENTATION — pii flows globally in milliseconds. anonymize.solutions addresses this through 100% EU hosting (Hetzner Germany, ISO 27001) with Self-Managed Docker deployment enabling data localization in any jurisdiction.

The Problem

Only ~35 of 54 African countries have data protection laws. Variable enforcement. PII collected by telecoms, banks, government without constraint

Root cause: T7 — JURISDICTION FRAGMENTATION: PII flows globally in milliseconds.

The Solution: How anonymize.solutions Addresses This

Detection Capabilities

anonymize.solutions identifies 260+ entity types including telecom subscriber data, banking records, government IDs, biometric registrations. The dual-layer (regex + NLP) architecture uses 210+ custom pattern recognizers (246 patterns, 75+ country formats, checksum-validated) for structured identifiers and spaCy (25 languages) + Stanza (7 languages) + XLM-RoBERTa (16 languages) for contextual references.

Anonymization Methods

Redact is recommended: anonymizing data collected by telecoms, banks, and governments prevents misuse where data protection laws are absent. Encrypt provides an alternative — AES-256-GCM encryption provides reversible protection where complete anonymization may not be legally required.

Architecture & Deployment

Self-Managed deployment (Docker containers, air-gapped option) eliminates cloud dependency entirely. Managed Private provides dedicated EU infrastructure with customer-managed encryption keys.

Structural Limits

This pain point stems from JURISDICTION FRAGMENTATION, a structural dynamic that no technology can fully resolve. Within these limits, anonymize.solutions provides targeted mitigations: Only ~35 of 54 African countries have data protection laws. Self-Managed deployment (Docker) enables organizations to implement anonymization standards exceeding local requirements.

Compliance Mapping

This pain point intersects with African Union Malabo Convention, national data protection laws where they exist. anonymize.solutions’s GDPR, HIPAA, FERPA, PCI-DSS, ISO 27001 compliance coverage, combined with 100% EU (Hetzner Germany, ISO 27001) hosting, provides documented technical measures for regulatory submissions.

05. ePrivacy stalemate

Evidence refs: 2.10

Executive Summary

ePrivacy stalemate represents a critical privacy challenge: Pre-smartphone rules governing smartphone communications since 2017. This pain point is driven by JURISDICTION FRAGMENTATION — pii flows globally in milliseconds. anonymize.solutions addresses this through 100% EU hosting (Hetzner Germany, ISO 27001) with Self-Managed Docker deployment enabling data localization in any jurisdiction.

The Problem

Pre-smartphone rules governing smartphone communications since 2017. Nine years of stalemate from industry lobbying. 2002 Directive still in effect

Root cause: T7 — JURISDICTION FRAGMENTATION: PII flows globally in milliseconds.

The Solution: How anonymize.solutions Addresses This

Detection Capabilities

anonymize.solutions identifies 260+ entity types including cookie identifiers, tracking pixels, device fingerprints, communication metadata. The dual-layer (regex + NLP) architecture uses 210+ custom pattern recognizers (246 patterns, 75+ country formats, checksum-validated) for structured identifiers and spaCy (25 languages) + Stanza (7 languages) + XLM-RoBERTa (16 languages) for contextual references.

Anonymization Methods

Redact is recommended: anonymizing tracking data regardless of ePrivacy status provides protection not dependent on resolving a nine-year regulatory stalemate. Replace provides an alternative — substituting tracking identifiers enables compliance with both the 2002 Directive and any future ePrivacy Regulation. For reversibility, Encrypt (AES-256-GCM) enables authorized recovery.

Architecture & Deployment

100% EU hosting (Hetzner Germany, ISO 27001) satisfies GDPR data residency. Self-Managed deployment (Docker) enables data localization in any jurisdiction. Compliance spans GDPR, HIPAA, FERPA, PCI-DSS, ISO 27001.

Structural Limits

This pain point stems from JURISDICTION FRAGMENTATION, a structural dynamic that no technology can fully resolve. Within these limits, anonymize.solutions provides targeted mitigations: Nine years of ePrivacy stalemate from industry lobbying is a jurisdictional failure. The platform enables organizations to anonymize tracking data now, under both current and future regulatory requirements.

Compliance Mapping

This pain point intersects with ePrivacy Directive 2002/58/EC, proposed ePrivacy Regulation, GDPR Article 95. anonymize.solutions's GDPR, HIPAA, FERPA, PCI-DSS, ISO 27001 compliance coverage, combined with 100% EU (Hetzner Germany, ISO 27001) hosting, provides documented technical measures for regulatory submissions.

06. Data localization dilemma

Evidence refs: 7.8

Executive Summary

Data localization dilemma represents a critical privacy challenge: African/MENA/Asian PII stored in US/EU data centers. This pain point is driven by JURISDICTION FRAGMENTATION — pii flows globally in milliseconds. anonymize.solutions addresses this through 100% EU hosting (Hetzner Germany, ISO 27001) with Self-Managed Docker deployment enabling data localization in any jurisdiction.

The Problem

African/MENA/Asian PII stored in US/EU data centers. Subject to CLOUD Act. But local storage in weak-rule-of-law countries may reduce protection

Root cause: T7 — JURISDICTION FRAGMENTATION: PII flows globally in milliseconds.

The Solution: How anonymize.solutions Addresses This

Detection Capabilities

anonymize.solutions identifies 260+ entity types including data center location identifiers, cloud provider metadata, transfer records. The dual-layer (regex + NLP) architecture uses 210+ custom pattern recognizers (246 patterns, 75+ country formats, checksum-validated) for structured identifiers and spaCy (25 languages) + Stanza (7 languages) + XLM-RoBERTa (16 languages) for contextual references.

Anonymization Methods

Redact is recommended: anonymizing data at collection eliminates the localization dilemma — anonymized data does not require localization. Encrypt provides an alternative — AES-256-GCM with locally-managed keys enables secure storage in any data center while maintaining organizational control.

Architecture & Deployment

Self-Managed deployment (Docker containers, air-gapped option) eliminates cloud dependency entirely. Managed Private provides dedicated EU infrastructure with customer-managed encryption keys.

Structural Limits

This pain point stems from JURISDICTION FRAGMENTATION, a structural dynamic that no technology can fully resolve. Within these limits, anonymize.solutions provides targeted mitigations: Data localization creates a dilemma: US hosting subjects data to CLOUD Act, local hosting in weak-rule-of-law countries may reduce protection. Self-Managed deployment resolves this.

Compliance Mapping

This pain point intersects with GDPR Article 44 transfer restrictions, national data localization requirements. anonymize.solutions’s GDPR, HIPAA, FERPA, PCI-DSS, ISO 27001 compliance coverage, combined with 100% EU (Hetzner Germany, ISO 27001) hosting, provides documented technical measures for regulatory submissions.

07. Whistleblower jurisdiction shopping

Evidence refs: 12.10

Executive Summary

Whistleblower jurisdiction shopping represents a critical privacy challenge: Five Eyes intelligence sharing bypasses per-country protections. This pain point is driven by JURISDICTION FRAGMENTATION — pii flows globally in milliseconds. anonymize.solutions addresses this through 100% EU hosting (Hetzner Germany, ISO 27001) with Self-Managed Docker deployment enabling data localization in any jurisdiction.

The Problem

Five Eyes intelligence sharing bypasses per-country protections. Source in Country A, org in Country B, server in Country C — three legal regimes, weakest wins

Root cause: T7 — JURISDICTION FRAGMENTATION: PII flows globally in milliseconds.

The Solution: How anonymize.solutions Addresses This

Detection Capabilities

anonymize.solutions identifies 260+ entity types including source identifiers, whistleblower documents, cross-jurisdictional evidence. The dual-layer (regex + NLP) architecture uses 210+ custom pattern recognizers (246 patterns, 75+ country formats, checksum-validated) for structured identifiers and spaCy (25 languages) + Stanza (7 languages) + XLM-RoBERTa (16 languages) for contextual references.

Anonymization Methods

Redact is recommended: anonymizing source-identifying information before documents cross jurisdictions prevents weakest-link exploitation. Replace provides an alternative — substituting source identifiers enables document sharing across jurisdictions without exposing source identity. For reversibility, Encrypt (AES-256-GCM) enables authorized recovery.

Architecture & Deployment

Self-Managed deployment (Docker containers, air-gapped option) eliminates cloud dependency entirely. Managed Private provides dedicated EU infrastructure with customer-managed encryption keys.

Structural Limits

This pain point stems from JURISDICTION FRAGMENTATION, a structural dynamic that no technology can fully resolve. Within these limits, anonymize.solutions provides targeted mitigations: Five Eyes intelligence sharing bypasses per-country protections. Self-Managed deployment combined with document anonymization provides the strongest available protection.

Compliance Mapping

This pain point intersects with EU Whistleblower Directive, press freedom laws, Five Eyes agreements. anonymize.solutions’s GDPR, HIPAA, FERPA, PCI-DSS, ISO 27001 compliance coverage, combined with 100% EU (Hetzner Germany, ISO 27001) hosting, provides documented technical measures for regulatory submissions.

T7 JURISDICTION FRAGMENTATION — Case Study 8 of 10

08. DP regulatory uncertainty

Evidence refs: 14.8

Executive Summary

DP regulatory uncertainty represents a critical privacy challenge: No regulator has formally endorsed differential privacy as satisfying anonymization requirements. This pain point is driven by JURISDICTION FRAGMENTATION — pii flows globally in milliseconds. anonymize.solutions addresses this through 100% EU hosting (Hetzner Germany, ISO 27001) with Self-Managed Docker deployment enabling data localization in any jurisdiction.

The Problem

No regulator has formally endorsed differential privacy as satisfying anonymization requirements. Organizations invest in DP with uncertain legal status

Root cause: T7 — JURISDICTION FRAGMENTATION: PII flows globally in milliseconds.

The Solution: How anonymize.solutions Addresses This

Detection Capabilities

anonymize.solutions identifies 260+ entity types including DP outputs, epsilon parameters, aggregate statistics, privacy budget records. The dual-layer (regex + NLP) architecture uses 210+ custom pattern recognizers (246 patterns, 75+ country formats, checksum-validated) for structured identifiers and spaCy (25 languages) + Stanza (7 languages) + XLM-RoBERTa (16 languages) for contextual references.

Anonymization Methods

Redact is recommended: anonymizing PII using established methods provides legal certainty that DP currently lacks — regulators endorse anonymization but not DP. Hash provides an alternative — deterministic hashing provides recognized anonymization with clear legal status, unlike DP in regulatory uncertainty. For reversibility, Encrypt (AES-256-GCM) enables authorized recovery.

Architecture & Deployment

100% EU hosting (Hetzner Germany, ISO 27001) satisfies GDPR data residency. Self-Managed deployment (Docker) enables data localization in any jurisdiction. Compliance spans GDPR, HIPAA, FERPA, PCI-DSS, ISO 27001.

Structural Limits

This pain point stems from JURISDICTION FRAGMENTATION, a structural dynamic that no technology can fully resolve. Within these limits, anonymize.solutions provides targeted mitigations: No regulator has endorsed DP as satisfying anonymization. The platform provides methods with established legal recognition, avoiding regulatory uncertainty.

Compliance Mapping

This pain point intersects with GDPR Recital 26 anonymization standard, Article 29 Working Party opinion. anonymize.solutions's GDPR, HIPAA, FERPA, PCI-DSS, ISO 27001 compliance coverage, combined with 100% EU (Hetzner Germany, ISO 27001) hosting, provides documented technical measures for regulatory submissions.

09. Surveillance tech export

Evidence refs: 4.2

Executive Summary

Surveillance tech export represents a critical privacy challenge: NSO Group (Israel) sells Pegasus found in 45+ countries — Saudi Arabia, Mexico, India, Hungary. This pain point is driven by JURISDICTION FRAGMENTATION — pii flows globally in milliseconds. anonymize.solutions addresses this through 100% EU hosting (Hetzner Germany, ISO 27001) with Self-Managed Docker deployment enabling data localization in any jurisdiction.

The Problem

NSO Group (Israel) sells Pegasus found in 45+ countries — Saudi Arabia, Mexico, India, Hungary. Export controls weak, enforcement weaker, accountability zero

Root cause: T7 — JURISDICTION FRAGMENTATION: PII flows globally in milliseconds.

The Solution: How anonymize.solutions Addresses This

Detection Capabilities

anonymize.solutions identifies 260+ entity types including surveillance target identifiers, spyware indicators, Pegasus artifacts. The dual-layer (regex + NLP) architecture uses 210+ custom pattern recognizers (246 patterns, 75+ country formats, checksum-validated) for structured identifiers and spaCy (25 languages) + Stanza (7 languages) + XLM-RoBERTa (16 languages) for contextual references.

Anonymization Methods

Redact is recommended: anonymizing surveillance research documents prevents identification of targets and journalists investigating spyware proliferation. Encrypt provides an alternative — AES-256-GCM enables secure collaboration among researchers investigating surveillance entities across jurisdictions.

Architecture & Deployment

Self-Managed deployment (Docker containers, air-gapped option) eliminates cloud dependency entirely. Managed Private provides dedicated EU infrastructure with customer-managed encryption keys.

Structural Limits

This pain point stems from JURISDICTION FRAGMENTATION, a structural dynamic that no technology can fully resolve. Within these limits, anonymize.solutions provides targeted mitigations: Surveillance technology in 45+ countries with weak export controls is a jurisdictional failure. Air-gapped processing ensures research documents never transit compromised networks.

Compliance Mapping

This pain point intersects with EU Dual-Use Regulation, Wassenaar Arrangement, human rights legislation. anonymize.solutions’s GDPR, HIPAA, FERPA, PCI-DSS, ISO 27001 compliance coverage, combined with 100% EU (Hetzner Germany, ISO 27001) hosting, provides documented technical measures for regulatory submissions.

10. Government PII purchasing

Evidence refs: 1.5

Executive Summary

Government PII purchasing represents a critical privacy challenge: ICE, IRS, DIA buy location data from brokers. This pain point is driven by JURISDICTION FRAGMENTATION — pii flows globally in milliseconds. anonymize.solutions addresses this through 100% EU hosting (Hetzner Germany, ISO 27001) with Self-Managed Docker deployment enabling data localization in any jurisdiction.

The Problem

ICE, IRS, DIA buy location data from brokers. Purchasing what they cannot legally collect. Third-party doctrine loophole converts commercial data into government surveillance

Root cause: T7 — JURISDICTION FRAGMENTATION: PII flows globally in milliseconds.

The Solution: How anonymize.solutions Addresses This

Detection Capabilities

anonymize.solutions identifies 260+ entity types including location data, broker records, government purchase orders, third-party doctrine data. The dual-layer (regex + NLP) architecture uses 210+ custom pattern recognizers (246 patterns, 75+ country formats, checksum-validated) for structured identifiers and spaCy (25 languages) + Stanza (7 languages) + XLM-RoBERTa (16 languages) for contextual references.

Anonymization Methods

Redact is recommended: anonymizing location data before it reaches commercial datasets closes the third-party doctrine loophole — agencies cannot buy what is anonymized. Hash provides an alternative — hashing identifiers enables analytical value while preventing government purchasing of individual-level data. For reversibility, Encrypt (AES-256-GCM) enables authorized recovery.

Architecture & Deployment

The REST API integrates into data pipelines (n8n, Make, Zapier) for automated PII anonymization before data reaches downstream systems. Three deployment models — SaaS (token pay-per-use), Managed Private (customer key management), and Self-Managed (Docker, air-gapped) — match any infrastructure requirement.

Structural Limits

This pain point stems from JURISDICTION FRAGMENTATION, a structural dynamic that no technology can fully resolve. Within these limits, anonymize.solutions provides targeted mitigations: Government agencies buying what they cannot legally collect is a fundamental jurisdictional exploit. Anonymizing data before it reaches commercial datasets reduces individual-level data available for purchase.

Compliance Mapping

This pain point intersects with Fourth Amendment, GDPR Article 6, proposed Fourth Amendment Is Not For Sale Act. anonymize.solutions's GDPR, HIPAA, FERPA, PCI-DSS, ISO 27001 compliance coverage, combined with 100% EU (Hetzner Germany, ISO 27001) hosting, provides documented technical measures for regulatory submissions.

Product Specifications

Product Version v1.6.12

Entity Types 260+

Detection Layers Dual-layer: 210+ regex recognizers + 3 NLP engines

Languages 48 (spaCy 25, Stanza 7, XLM-RoBERTa 16)

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

Deployment Options SaaS, Managed Private, Self-Managed (Docker/Air-Gapped)

Integration Points REST API, MCP Server, Office Add-in, Desktop App, Chrome Extension

Hosting 100% EU (Hetzner Germany, ISO 27001)

Compliance GDPR, HIPAA, FERPA, PCI-DSS, ISO 27001

Other Products Addressing This Transistor

- anonym.legal (Cloud platform)

Online versions available at:
https://anonym.community/anonymize.solutions/