Consent Architecture: DKMS as the Structurally Sound Foundation for EHDS Article 71

Vereign AG

2026-04-29

Consent-Architektur: DKMS als strukturell tragfähige Grundlage für EHDS Article 71

Vereign AG — April 2026

1. Zusammenfassung

Das europäische Gesundheitsdatenrecht hat eine Schwelle überschritten. Opt-out ist keine unverbindliche Absichtserklärung mehr — unter EHDS Article 71 ist es ein **gesetzliches Recht** der natürlichen Person, durchsetzbar in jedem Mitgliedstaat, der identifizierbare Gesundheitsdaten zur Sekundärnutzung verarbeitet. In Verbindung mit GDPR Articles 7(3) und 17(2), eIDAS 2.0 Article 5a, dem Schweizer DSG und HFG sowie dem deutschen PDSG konvergieren fünf unabhängige Rechtsordnungen auf einen einzigen Satz von technischen Invarianten: **personenbezogene Kennungen, überprüfbarer zeitgestempelter Opt-out, Reversibilität ohne Re-Identifizierung, controllerübergreifende Weitergabe und Nicht-Verknüpfbarkeit**. Zentralisiertes PKI und föderierte Identität erfüllen höchstens eine oder zwei dieser Anforderungen; X.509 erfüllt keine davon auf der Bürgerebene. **Dezentrales Schlüsselmanagement (DKMS) ist die erste strukturell tragfähige Grundlage, um Opt-out durchgängig zu wahren — in organisationsübergreifenden, nach der Offenlegung wirksamen, regulatorisch beaufsichtigten Konstellationen.** Die These hat klare Grenzen: Derivate, die das System vor dem Widerruf verlassen haben, unveränderliche Sicherungen und einzelne unkooperative Gegenparteien bleiben architektonisch unerreichbar.

Das Vergleichsdossier 2025–2026 (Kaiser USD 47,5 Mio., Sutter USD 21,5 Mio., parallele Klagen gegen BJC, Northwell, Catholic Health, Aspirus und SSM Health) ist der Frühindikator: Jeder zentralisierte Vorfall teilt ein Merkmal — die Nutzenden hatten keine architektonische Handlungsmacht.

---

2. Warum jetzt — regulatorische Konvergenz in 24 Monaten

Zwei Jahrzehnte lang behandelte das Consent-Management im Gesundheits-IT-Bereich Opt-out als UX-Problem. Ab 2024 konvergierten fünf unabhängige Rechtsordnungen auf dasselbe technische Muster und liessen Anbietern Monate — nicht Jahre — um strukturelle Compliance nachzuweisen.

EHDS Article 71 — Regulation (EU) 2025/327. Angenommen am 11. Februar 2025; veröffentlicht im Amtsblatt der Europäischen Union (ABl. L 2025/327) am 5. März 2025; in Kraft seit dem 26. März 2025. Article 71(1) gibt jeder natürlichen Person das Recht, der Sekundärverarbeitung identifizierbarer elektronischer Gesundheitsdaten zu widersprechen. Article 71(2) untersagt neue Datengenehmigungen für identifizierbare Daten nach Ausübung des Opt-out, lässt jedoch zuvor erteilte Genehmigungen bestehen. **Article 71(8)** verbietet Dateninhabern, zusätzliche Identifizierungsdaten ausschliesslich zur Wahrung des Opt-out zu beschaffen — der technische Wendepunkt, der das naheliegende Muster eines «zentralen Registers der Opt-out-Personen» ausschliesst.

GDPR Articles 7(3) und 17(2) — Regulation (EU) 2016/679. Article 7(3) verlangt, dass der Widerruf der Einwilligung «ebenso einfach wie die Erteilung» sein muss. Article 17(2) begründet eine Weitergabepflicht: Ein Verantwortlicher, der einem Löschungsantrag nachkommt, muss «angemessene Massnahmen einschliesslich technischer Massnahmen ergreifen», um nachgelagerte Verantwortliche zu informieren. Article 9(2)(a) erhöht die Anforderungen für Gesundheitsdaten auf *ausdrückliche* Einwilligung; Article 17(3)(c)/(d) sieht Ausnahmen für die öffentliche Gesundheitsversorgung und Forschung vor, die eine wörtliche Löschung der meisten klinischen Daten strukturell unerreichbar machen — genau deshalb hat EHDS das Recht als **Vorwärts-Unterdrückung** (Forward Suppression) und nicht als rückwirkende Löschung ausgestaltet.

eIDAS 2.0 — Regulation (EU) 2024/1183. Ändert Regulation (EU) 910/2014 zur Einführung der Europäischen Digitalen Identitätsbrieftasche (EUDIW). Article 5a(14) schreibt «vollständige Benutzerkontrolle» über Wallet-Vorgänge vor. Article 5a(16)(a) verbietet die kontextübergreifende Verfolgung der Wallet-Nutzung; Article 5a(16)(b) schreibt **Nicht-Verknüpfbarkeit** zwischen Credential-Präsentationen bei verschiedenen Verifizierern vor. Zusammen sind 5a(16)(a)–(b) die operative Form von EHDS Article 71(8): Eine Architektur, in der der Betreiber Bürgerinnen und Bürger über Verifizierer hinweg korrelieren kann, scheitert per Definition am Test der Nicht-Verknüpfbarkeit.

Schweizer DSG und HFG. Das revidierte Bundesgesetz über den Datenschutz (DSG / nDSG, SR 235.1, in Kraft seit dem 1. September 2023) verlangt ausdrückliche Einwilligung für besonders schützenswerte Daten in Article 6(6) sowie ein absolutes Widerrufsrecht in Article 6(7), wobei das Löschungsrecht in Article 32 Aufbewahrungspflichten unterliegt. Das Humanforschungsgesetz (HFG / HRA, SR 810.30) gewährt in Article

7(2) und Article 17 das Recht auf Widerruf der Einwilligung und Widerspruch gegen die Weiternutzung von Gesundheitsdaten. Das künftige EGDG (Botschaft des Bundesrates, 5. November 2025) kehrt das EPD-Modell von Opt-in auf Opt-out um, mit geplantem Inkrafttreten ca. 2028–2030; das BDG (DigiSanté-Rechtsgrundlage für die Sekundärnutzung) befindet sich in der Ausarbeitung. Die kantonsübergreifende Weitergabe macht den Schweizer Fall strukturell anspruchsvoller als den EU-Fall.

Deutsches PDSG. Das Patientendaten-Schutz-Gesetz operationalisiert die Opt-out-Architektur der deutschen elektronischen Patientenakte (ePA), die seit Januar 2025 für rund 73 Millionen gesetzlich Versicherte in Betrieb ist. Das PDSG kodifiziert die Mechanik der Vorwärts-Unterdrückung — Versicherte, die der ePA widersprechen, dürfen nicht auf der Grundlage des Opt-in verarbeitet werden — für eine Bevölkerung, die grösser ist als die meisten EU-Mitgliedstaaten zusammen. Der nationale Umsetzungsdruck auf die Consent-Architektur ist daher nicht theoretischer Natur; er ist im grössten Einzahler-Gesundheitswesen Europas bereits operativ wirksam.

Die TEHDAS2-Entwurfsrichtlinie der Joint Action (September 2025) bestätigt, dass der technische Mechanismus der Opt-out-Weitergabe durch das EU-Recht selbst **nicht** vorgegeben wird und der Umsetzung der Mitgliedstaaten überlassen bleibt. Das ist die architektonische Schwachstelle: Jeder Staat könnte seinen eigenen Ansatz wählen, doch nur ein subjektkontrolliertes Schlüsselkonzept erfüllt Article 71(8), ohne ein verbotenes Re-Identifizierungsregister einzuführen. Anbieter, die in einem Mitgliedstaat eine konforme Architektur liefern, werden in allen siebenundzwanzig verkaufen; Anbieter, die nur die lokale UX lösen, werden in jeder Transposition mit einer anderen architektonischen Diskussion konfrontiert.

Jede dieser fünf Rechtsordnungen für sich allein ist handhabbar. **Alle fünf zusammen, in einem 24-Monats-Fenster, sind die architektonische Zäsur.** Anbieter im Gesundheits-IT-Bereich stehen nun vor einem Markt, in dem «Consent-Management» durchgängig, über Grenzen, über Verantwortliche und über die Zeit hinweg zusammenwirken muss — und das zentralisierte Registermodell, das die Branche zwei Jahrzehnte lang getragen hat, ist durch das primäre Recht des grössten Wirtschaftsblocks der Welt ausgeschlossen.

---

3. Die fünf technischen Invarianten

Die fünf Rechtsordnungen konvergieren auf einen kleinen, präzisen Satz technischer Anforderungen. Diese sind keine Absichtserklärungen — sie sind testbare Prädikate, anhand derer jede Consent-Architektur bewertet werden kann.

3.1 Personenbezogene Kennungen

Die betroffene Person muss die Kennung kontrollieren, unter der ihre Genehmigungen, Autorisierungen und ihr Consent-Status referenziert werden. Dies ist die *Voraussetzung* für jede andere Invariante: Besitzt der Betreiber die Kennung, besitzt er den Opt-out. EHDS Article 71(8) schliesst betreiberseitige Re-Identifizierungsregister ausdrücklich aus; das Mandat zur «vollständigen Benutzerkontrolle» in eIDAS 2.0 Article 5a(14) benennt dieselbe Eigenschaft auf der Wallet-Ebene. Ohne eine subjektbezogene Kennung kollabieren Weitergabe, Reversibilität und Nicht-Verknüpfbarkeit allesamt zu Betreiberpolitik.

3.2 Überprüfbarer zeitgestempelter Opt-out

Für jede Datengenehmigung muss das System den genauen Zeitpunkt der Erteilung und den genauen Zeitpunkt des Widerrufs kennen — und eine dritte Partei (Aufsichtsbehörde, Gericht, nachgelagerter Verantwortlicher) muss beides verifizieren können, ohne den Protokollen des Betreibers zu vertrauen. EHDS Article 71(2) zieht eine scharfe zeitliche Grenze: Vor dem Opt-out erteilte Genehmigungen bleiben gültig; danach erteilte sind rechtswidrig. Dies ist ohne eine manipulationssichere, durch Dritte verifizierbare Zeitleiste des Consent-Status der betroffenen Person nicht durchsetzbar.

3.3 Reversibilität ohne Re-Identifizierung

Recital 54 der EHDS-Verordnung bestätigt, dass der Opt-out reversibel ist (Bürgerinnen und Bürger können wieder einwilligen) und formfrei (keine Mindestdauer). Article 71(8) verbietet dem Dateninhaber, zusätzliche Identifizierungsdaten ausschliesslich zur Wahrung des Opt-out zu beschaffen. Beide Klauseln zusammen ergeben eine enge Anforderung: Das System muss das Kippen des Consent-Status nach Belieben der betroffenen Person unterstützen — **ohne** dass der Dateninhaber ein paralleles Re-Identifizierungsregister aufbaut, um nachzuverfolgen, wer welchen Weg gewählt hat. Jede Architektur, die ein «einfaches Register der Opt-out-Personen» erfordert, verstösst direkt gegen Article 71(8).

3.4 Controllerübergreifende Weitergabe

GDPR Article 17(2) verlangt, dass der Verantwortliche, der einem Löschungsantrag nachkommt, «angemessene Massnahmen einschliesslich technischer Massnahmen» ergreift, um nachgelagerte Verantwortliche zu informieren, die Kopien, Replikate oder Verknüpfungen besitzen. EHDS Article 71, angewandt auf Multi-Controller-Genehmigungsketten, verschärft dies: Das Opt-out-Signal muss jede Health Data Access Body, jedes Forschungskonsortium und jeden Unterauftragsverarbeiter erreichen, der Daten auf der Grundlage einer früheren Genehmigung erhalten hat. Die Weitergabe darf kein Papierregister sein — sie muss ein überprüfbares Artefakt sein, das nachgelagerte Parteien erneut überprüfen können.

3.5 Nicht-Verknüpfbarkeit

eIDAS 2.0 Article 5a(16)(b) schreibt Nicht-Verknüpfbarkeit zwischen Präsentationen desselben Credentials bei verschiedenen Verifizierern vor. Die praktische Konsequenz: Eine Architektur, in der eine einzige Partei (selbst ein autorisierter Intermediär) alle Transaktionen über Verifizierer hinweg einsehen kann, scheitert per Konstruktion am Test. Diese Eigenschaft schliesst föderierte Identitätsanbieter von der Bürgerebene EHDS-konformer Systeme aus: Der IdP sieht per Design jeden Login und jede Credential-Präsentation. Föderierung kann Weitergabe erfüllen, jedoch nur unter Verletzung der Nicht-Verknüpfbarkeit.

Diese fünf Invarianten bilden ein zusammenhängendes System. **X.509 PKI erfüllt keine davon auf der Bürgerebene. Föderierte IdPs erfüllen die Weitergabe-Invariante nur unter Verletzung der Nicht-Verknüpfbarkeit. DKMS erfüllt alle fünf.** Das ist der Anspruch auf strukturelle Tragfähigkeit, und der Rest dieses Dokuments untersucht ihn.

4. Die Falle von Article 71(8)

Das einfachste Implementierungsmuster für Opt-out — das, das ein Gesundheits-IT-Anbieter in der ersten Stunde des Architekturgesprächs entwerfen wird — ist **ein zentrales Register der abgemeldeten Bürger-IDs**. Jeder Dateninhaber fragt das Register ab, bevor er verarbeitet; befindet sich die ID der betroffenen Person auf der Liste, wird die Verarbeitung gestoppt. Einfach. Vertraut. Prüfbar.

Article 71(8) schliesst dieses Muster vollständig aus.

Die Klausel verbietet Dateninhabern, zusätzliche Identifizierungsdaten ausschliesslich zur Wahrung des Opt-out zu beschaffen. **Die «Liste der Opt-out-IDs» ist per Konstruktion genau ein solches Register.** Sie existiert für keinen anderen Zweck als die Re-Identifizierung von Bürgerinnen und Bürgern im Negativfall — um festzustellen, dass *diese Person den Opt-out ausgeübt hat und daher nicht verarbeitet werden darf*. Die Liste selbst ist der Verstoss gegen die Regel, die sie verhindern soll.

Die Falle ist rekursiv. Jeder Versuch, das Register zu anonymisieren (IDs hashen, pseudonymisieren, in einer separaten Trust Domain aufbewahren) reaktiviert das ursprüngliche Problem: Der Dateninhaber benötigt *irgendeine* Kennung zum Abgleich mit der Liste, und diese Kennung muss aus den Daten ableitbar sein, die der Inhaber bereits besitzt. Der Hash ist für den Inhaber, der die Eingabe kennt, nicht anonym; das Pseudonym ist für den Inhaber, der die Verknüpfung kennt, nicht anonym. Recital 54 verstärkt dies, indem er vorschreibt, dass der Opt-out reversibel und formfrei ist — das Register muss also das Kippen des Status unterstützen, was wiederum erfordert, dass das Register verfolgt, *welche* Person *wann* gewechselt hat — genau der Re-Identifizierungsdatensatz, den Article 71(8) verbietet.

Die Konsequenz für Gesundheits-IT-Anbieter ist eindeutig. **Jedes «Consent-Management-Modul», dessen Architektur auf einer zentralen autoritativen Liste abgemeldeter Personen beruht, ist durch das primäre EU-Recht ausgeschlossen.** Dies ist keine UX-Designentscheidung; es ist der Unterschied zwischen einer Architektur, die EHDS einhalten kann, und einer, die es nicht kann. Generische Consent-Management-Produkte, die auf dem Registermuster aufgebaut sind — ob SaaS, On-Premises oder hybrid — werden bei jeder Transposition durch Mitgliedstaaten auf diese Anforderung stossen. Die strukturelle Antwort muss die Kennung unter die Kontrolle der betroffenen Person stellen, so dass der Dateninhaber kein Re-Identifizierungsregister führen muss.

---

5. Die DKMS-These

> **Dezentrales Schlüsselmanagement ist die erste strukturell tragfähige Grundlage, um Opt-out durchgängig zu wahren — in organisationsübergreifenden, nach der Offenlegung wirksamen, regulatorisch beaufsichtigten Konstellationen.**

DKMS — aufgebaut auf KERI, einer offenen Spezifikation der Trust over IP Foundation — verankert den Trust Root bei der betroffenen Person statt bei einer zentralisierten Autorität. Die betroffene Person (oder ihr Wallet-Agent) besitzt einen Autonomic IDentifier (AID), der selbstzertifizierend ist: Er wird von einem öffentlichen Schlüssel unter der Kontrolle der betroffenen Person abgeleitet, und seine Authentizität hängt nicht von einem Registrar ab. Alle den Dateninhabern, Verarbeitern und nachgelagerten Verantwortlichen erteilten Autorisierungen sind über ein Key Event Log (KEL) — ein nur anhängendes, durch Dritte überprüfbares Protokoll des Schlüsselstatus der betroffenen Person, einschliesslich Schlüsselrotationen — an diesen AID gebunden.

Widerruf ist in diesem Modell kein Antrag, der an einen Betreiber gestellt wird. Es ist eine **Schlüsselrotation, die die betroffene Person einseitig vornimmt**. Die Rotation wird im KEL veröffentlicht; von diesem Moment an müssen alle nachgelagerten Parteien, die Credentials besitzen, die im Schlüsselstatus vor der Rotation verankert sind, sich gegenüber dem aktuellen Status der betroffenen Person neu authentifizieren, um die Verarbeitung fortzusetzen. Vor der Rotation erteilte Genehmigungen bleiben dort wirksam, wo die zugrunde liegende Rechtsgrundlage dies zulässt (in Übereinstimmung mit EHDS Article 71(2)); neue Genehmigungen können nicht auf der Grundlage des alten Schlüsselstatus erteilt werden, da dieser nicht mehr der kontrollierende Status der betroffenen Person ist. Die betroffene Person hat architektonisch — nicht nur verfahrensmässig — die künftige Autorisierung entzogen, und jede nachgelagerte Partei, die die veröffentlichte Rotation ignoriert, erzeugt Signaturen, die als veraltet prüfbar sind.

Abgleich mit den fünf Invarianten:

Invariante	**DKMS-Mechanismus**
Personenbezogene Kennungen	Der AID ist die selbstzertifizierende Kennung der betroffenen Person; kein betreiberseitiger Index erforderlich
Überprüfbarer zeitgestempelter Opt-out	KEL enthält manipulationssichere, zeitgestempelte Schlüsselereignisse
Reversibilität ohne Re-Identifizierung	Opt-back-in = Schlüsselrotation zur Wiederherstellung der Autorisierung; kein paralleles Register
Controllerübergreifende Weitergabe	KEL ist publizierbar; Verifizierer müssen über Trust Domains hinweg erneut prüfen
Nicht-Verknüpfbarkeit	Kontextspezifische AIDs und Selective-Disclosure-Credentials vermeiden verifiziererübergreifende Korrelation

Vergleich mit bestehenden Optionen:

X.509 PKI bindet die Identität an ein CA-ausgestelltes Zertifikat. Die betroffene Person besitzt den Trust Root nicht — die CA tut es. Die Sperrung wird vom Betreiber gesteuert (CRL/OCSP) und schlägt standardmässig still fehl. Kontextübergreifende Nicht-Verknüpfbarkeit fehlt strukturell — jede Zertifikatspräsentation ist über die Seriennummer, den Issuer DN und den Subject DN des Zertifikats mit derselben Person verknüpfbar. X.509 erfüllt auf der Bürgerebene *keine* der fünf Invarianten.

Föderiertes IAM (OIDC, SAML). Der Identity Provider ist per Design der kontextübergreifende Tracker, den eIDAS 2.0 Article 5a(16)(b) verbietet. Föderierung kann die controllerübergreifende Weitergabe erfüllen (ein Single Logout leert nachgelagerte Sitzungen), jedoch nur unter Verletzung der Nicht-Verknüpfbarkeit — jeder Login läuft über den IdP, der jede Relying Party sieht, die die betroffene Person besucht. Die Architektur kann höchstens drei Invarianten erfüllen, und nur auf Kosten der fünften.

Zentralisiertes KMS (AWS KMS, Azure Key Vault, GCP Cloud KMS). Hervorragend für Single-Tenant-Workloads. Die kryptografische Löschung gemäss NIST SP 800-88 §2.5 via Customer-Managed Keys ist ein regulatorisch anerkanntes Terminal-Erasure-Primitiv (EDPB Guidelines 01/2025; ENISA 2019 §4.2). Sobald jedoch Daten die Mandantengrenze überschreiten — in ein Forschungskonsortium, einen nachgelagerten Verantwortlichen, einen genehmigten Sekundärnutzungsempfänger —, bewirkt die Vernichtung des CMK durch den Betreiber nichts an der Kopie. Die controllerübergreifende Weitergabe bleibt ungelöst. Schrems II / EDPB Recommendations 01/2020 Use Case 3 eskaliert dies weiter: Der Datenimporteur darf per Definition die Schlüssel nicht besitzen.

DKMS ersetzt diese Stacks nicht — es besetzt den genauen architektonischen Platz, den sie nicht ausfüllen können. Zentralisiertes KMS für mandantenspezifische Löschung, X.509 für Sperrung auf TLS-Ebene, föderiertes IAM für sitzungsbezogene Einwilligung — und DKMS für die organisationsübergreifende Schicht nach der Offenlegung, in der EHDS Article 71 tatsächlich angesiedelt ist.

---

6. Wo zentralisierte Architekturen versagen

Die fünf Invarianten sind testbar. Jede wichtige zentralisierte Consent-Architektur versagt auf strukturell spezifische Weise.

6.1 X.509 PKI versagt bei allen fünf Invarianten auf der Bürgerebene

X.509 bindet die Identität an eine Zertifizierungsstelle. Die CA generiert das Zertifikat der betroffenen Person oder ko-signiert es, besitzt die Ausstellungsentscheidung und kontrolliert die Sperrung. Personenbezogene Kennungen scheitern an der Wurzel — die Signatur der CA ist die Vertrauensquelle, nicht die betroffene Person. Zeitgestempelter Opt-out wird vom Betreiber gesteuert (die betroffene Person stellt einen Sperrantrag; die CA entscheidet, ob und wann sie ihn veröffentlicht), und die Sperrung propagiert nur so schnell wie die CRL-Aktualisierungsfenster oder die Verfügbarkeit von OCSP-Respondern — beides scheitert in Browsern standardmässig still. Reversibilität ohne Re-Identifizierung scheitert, weil die Neuausstellung die CA verpflichtet, die Identität des Subjekts erneut zu validieren, was im Gesundheitskontext erfordert, dass die CA genau die Identifizierungsdaten erneut beschafft, die EHDS Article 71(8) dem Dateninhaber zu besitzen verbietet. Die controllerübergreifende Weitergabe hängt davon ab, dass alle Relying Parties CRLs/OCSP korrekt prüfen, was die Vorfälle bei DigiNotar und Comodo als operativ fragil erwiesen haben. Nicht-Verknüpfbarkeit ist strukturell unmöglich: Jedes X.509-Zertifikat trägt eine Seriennummer und einen Issuer DN, der jede Präsentation mit derselben Person verknüpft.

6.2 Föderiertes IAM (OIDC/SAML) verletzt Nicht-Verknüpfbarkeit per Definition

OIDC und SAML föderieren die Authentifizierung über einen Identity Provider, der die Beziehung zwischen der betroffenen Person und der Relying Party vermittelt. Jeder Login, den die betroffene Person gegenüber einem beliebigen Verifizierer durchführt, läuft über den IdP. Der IdP weiss, welche Person wann auf welchen Dienst zugegriffen hat. Dies ist keine Konfigurationsentscheidung oder ein Richtlinienverstoss — es ist die architektonische Funktion des IdP. eIDAS 2.0 Article 5a(16)(b) schreibt Nicht-Verknüpfbarkeit zwischen Präsentationen desselben Credentials bei verschiedenen Verifizierern vor; der föderierte IdP ist per Konstruktion der einzelne Punkt, an dem jede Präsentation korreliert wird. Föderierung kann echte controllerübergreifende Weitergabe liefern (Single Logout, OAuth Token Revocation, OIDC Back-Channel Logout) — der Preis ist jedoch die Verletzung der Nicht-Verknüpfbarkeits-Invariante bei jeder Credential-Präsentation, die der IdP vermittelt.

6.3 Zentralisiertes KMS kann controllerübergreifende Weitergabe nicht leisten

AWS KMS, Azure Key Vault und GCP Cloud KMS bieten prüfbare Schlüsselverwahrung, FIPS 140-2 L3 / 140-3-Backends, geplante Schlüsselvernichtung (`ScheduleKeyDeletion`, Soft-Delete + Purge, `DESTROY_SCHEDULED`) und Envelope-Verschlüsselung mit DEK/KEK-Trennung. Innerhalb eines einzelnen Mandanten ist dies ein vollständig ausreichendes GDPR Article 17-Löschungsprimitiv — NIST SP 800-88 §2.5 erkennt kryptografische Löschung ausdrücklich als Sanitisierungstechnik auf Purge-Niveau an, und EDPB Guidelines 01/2025 behandeln die Schlüsselverwahrung als ergebnisbestimmend dafür, ob Daten für einen bestimmten Empfänger anonym sind. Die Architektur funktioniert **innerhalb der Mandantengrenze**.

Sie überschreitet die Grenze nicht. Sobald die Daten rechtmässig in ein Forschungskonsortium, einen genehmigten nachgelagerten Verantwortlichen oder einen Unterauftragsverarbeiter in einer anderen Trust Domain kopiert worden sind, bewirkt die KMS-Vernichtung des Mandanten nichts an der Kopie. GDPR Article 17(2)-Weitergabe wird zu einer vertraglichen Pflicht — Papierarbeit, keine Architektur. Die Genehmigungsketten-Struktur von EHDS Article 71 macht diese Lücke strukturell statt beiläufig: Jede Genehmigung ist potenziell der Beginn einer Multi-Controller-Kette, und zentralisiertes CMK besitzt keine Möglichkeit, über den ersten Glied hinauszureichen.

---

7. Wo DKMS nicht liefert — kritische Betrachtung

Die These ist strukturell, nicht absolut. Klare Abgrenzungen machen das Argument verteidigbar; Überreichweite zerstört es. Die DKMS-These hat vier explizite Grenzen.

7.1 Derivate — EDPB Opinion 28/2024

Sobald Daten in ein Derivat umgewandelt worden sind — Analyse-Aggregate, ML-Modellgewichte, statistische Extrakte, bereits eingereichte regulatorische Berichte — bewirkt die Schlüsselvernichtung am Quell-Ciphertext nichts am Derivat. EDPB Opinion 28/2024 zu Datenschutzaspekten von KI-Modellen (angenommen am 17. Dezember 2024) bestätigt ausdrücklich, dass Löschungspflichten sich nicht sauber auf Modellgewichte übertragen, sobald das Training stattgefunden hat. DKMS schneidet hier nicht besser ab als zentralisiertes CMK. Hat ein genehmigtes Forschungskonsortium ein Modell auf Daten trainiert, von denen sich die betroffene Person später abmeldet, bleiben die Modellgewichte bestehen. Der architektonische Beitrag ist die Prüfbarkeit der Ableitungskette, nicht das rückwirkende Rückgängigmachen der Ableitung.

7.2 Bereits erstellte Sicherungen

Keine Architektur mit Live-Schlüsselsperrung — ob DKMS oder zentralisiert — kann bereits auf unveränderliche Sicherungsmedien replizierte Daten zurückrufen. Offline-Sicherungen, die vor dem Widerruf erstellt wurden, befinden sich ausserhalb des Live-Schlüsselbereichs. Die pragmatische Antwort ist eine dokumentierte, geplante Schlüsselvernichtung in einem bekannten Aufbewahrungsfenster — die ICO-, CNIL- und BfDI-Leitlinien allesamt als ausreichend für in Sicherungen verbliebene personenbezogene Daten anerkennen. DKMS fügt sich in diese Disziplin ein; es ersetzt sie nicht.

7.3 Einzelne unkooperative Gegenpartei

In einem N-Parteien-Netzwerk mit einer Partei, die die veröffentlichte Schlüsselrotation ignoriert und weiterhin auf der Grundlage veralteter Credentials handelt, bietet DKMS **forensische Erkennung** — die veralteten Signaturen sind über das veröffentlichte Rotationsereignis hinaus prüfbar — jedoch keine **Prävention**. Ein vollständig nicht kooperierender nachgelagerter Verarbeiter, der Klartext exfiltriert und ausserhalb der verschlüsselten Hülle speichert, liegt architektonisch ausserhalb der Reichweite jedes Schlüsselmanagementsystems. DKMS stärkt die Beweisposition der Aufsichtsbehörde; es behebt die zugrunde liegende Nicht-Kooperation nicht. Im Vergleich zu einem vertraglich gut geregelten zentralisierten CMK-Bestand stärkt DKMS die Erkennung, ohne die Notwendigkeit vertraglicher, behördlicher oder gerichtlicher Durchsetzung gegen unkooperative Akteure zu beseitigen.

7.4 Single-Tenant-Workloads

Für Workloads, die vollständig innerhalb einer einzigen Trust Domain verbleiben — unternehmensinterne Daten unter einem einzigen Verantwortlichen, Single-Tenant-SaaS mit mandantenspezifischem CMK, öffentliches Web-TLS unter CA/Browser Forum-24-Stunden-Sperr-SLOs — ist die kryptografische Löschung gemäss NIST SP 800-88 §2.5 via zentralisiertem CMK vollständig ausreichend. EDPB Guidelines 01/2025 und ENISA 2019 §4.2 erkennen beide die Schlüsselvernichtung als terminale Löschung innerhalb der Mandantengrenze an. **Das Hinzufügen von DKMS zu diesen Workloads bedeutet operativen Mehraufwand ohne architektonischen Nutzen.** Die ehrliche Antwort lautet: Für Single-Tenant-Szenarien funktioniert der zentralisierte Stack.

7.5 Die entscheidende Grenze

DKMS dominiert, wenn **alle vier** der folgenden Bedingungen erfüllt sind:

1. Daten überschreiten **mindestens zwei Trust Domains**.
2. Einwilligung muss **nach der Offenlegung erhalten bleiben** (d. h. die Verarbeitung setzt über die Grenze hinaus fort).
3. Die Aufsichtsbehörde behandelt **die Schlüsselverwahrung als ergebnisbestimmend** (Schrems II / EDPB Recommendations 01/2020 Use Case 3 / EHDS Article 71(8)).
4. Parteien setzen DKMS **durchgängig** ein (ein Verifizierer, der das KEL ignoriert, hebt die Kette auf).

Ausserhalb dieser vier Bedingungen ist zentralisiertes CMK die rationale Wahl — und dies zu sagen macht die DKMS-These stärker, nicht schwächer, weil es den Anspruch genau dort verortet, wo die Beweise ihn stützen. Der Anspruch lautet nicht, dass DKMS Cookie-Banner oder Single-Tenant-SaaS-Löschung löst. Der Anspruch lautet, dass DKMS die richtige strukturelle Wahl für *genau* jene Fälle ist, die für kantonsübergreifende, organisationsübergreifende, regulatorisch beaufsichtigte Consent-Verarbeitung im Gesundheitswesen nach der Offenlegung relevant sind.

---

8. Produktivbeweis

Vereign betreibt die DKMS-Architektur heute in der Produktion, mit expliziten Vorbehalten dazu, was ausgeliefert ist und was architektonisch geplant ist.

SEAL ist die produktive Kommunikationsschicht: verschlüsselte Swarm-Zustellung für ausgehende Kommunikation, mit nachrichtenspezifischen Schlüsseln und empfängerkontrollierter Entschlüsselung. SEAL übermittelt **800.000+ verifizierte Nachrichten monatlich** für institutionelle Nutzer — der massgebliche Produktivnachweis für die Architektur. Jede Nachricht nutzt dasselbe Schlüsselereignis-Substrat, das der Consent-These zugrunde liegt: subjektkontrolliertes Schlüsseln, durch Dritte verifizierbare Zeitstempel und kontextspezifische Nicht-Verknüpfbarkeit zwischen Empfängern.

Stargate — die AID-verankerte Autorisierungsschicht, in der Datengenehmigungen an das KEL der betroffenen Person gebunden sind — tritt ab Juni 2026 mit HIN als erstem operativem Einsatz in die frühe Produktion ein. Stargate ist die Consent-Oberfläche der These: An Dateninhaber erteilte Autorisierungen sind am AID der betroffenen Person verankert; Schlüsselrotationen durch die betroffene Person propagieren durch das KEL; nachgelagerte Verifizierer prüfen erneut. Der HIN-Einsatz ist ein Soft Launch im Umfang; die **Massenausroll-Erzählung ist für die Zeit nach Sommer 2026 reserviert**, nachdem der frühe Produktionskohort unter realen regulatorischen Bedingungen operative Belege gesammelt hat.

HIN-Brücken ermöglichen die Interoperabilität des Widerrufs mit X.509-nutzenden Gegenparteien über die KERI-verankerte S/MIME-Brücke, die in der E-Mail-Security-Wissensdatenbank dokumentiert ist. Dies ist die pragmatische Anerkennung, dass DKMS mit dem bestehenden X.509-Gesundheitswesen komponieren — nicht sofort ersetzen — wird.

FHIR-over-Stargate ist architektonisch — die Produktivbereitstellung hängt vom Onboarding der Spitäler ab; frühestens realistisch September 2026. Die architektonische Geschichte ist überzeugend: FHIR-Ressourcen, die durch Stargate fliessen, erben das AID-verankerte Autorisierungsmodell, sodass der Consent-Status auf Ressourcenebene dort liegt, wo die betroffene Person ihn kontrolliert. Die technische Umsetzung der Spitaladoption — Integration klinischer Systeme, regulatorische Abnahme, operative Governance — ist jedoch ein mehrquartaliges Vorhaben. Wir beanspruchen FHIR-over-Stargate nicht als ausgeliefert. Wir benennen es als den bewussten nächsten Schritt mit einem bekannten Frühesttermin und gehen davon aus, dass die operative Bereitstellung der architektonischen Bereitschaft um ein messbares Intervall nachhinkt. Beides zu verwechseln ist der Fehler, den dieses Dokument zu vermeiden sucht.

Die produktive Erfolgsbilanz ist relevant, weil sie diese These von einer Folienpräsentation unterscheidet. Technische Organisationen begegnen dem Argument Zentralisierung vs. Dezentralisierung routinemässig; was sie selten antreffen, ist Dezentralisierung, die in der Praxis, unter lebendiger institutioneller Regulierung und in einem regulierten Sektor eingesetzt wird. Das Substrat für verifiziertes Messaging trägt seit ausreichend langer Zeit echten institutionellen Verkehr, um die operativen Ecken von DKMS offenzulegen — Disziplin der Schlüsselrotation, organisationsübergreifende Erkennung, Aufbewahrung von Prüfprotokollen, Handlungsmacht der Empfänger — und diese Ecken wurden in der Produktion statt in der Theorie verfeinert. Wenn Stargate ab Juni 2026 in die frühe Produktion eintritt, wird es auf demselben Substrat laufen. Das architektonische Argument ist daher keine Prognose; es ist eine Extrapolation aus beobachtetem Betrieb in der Praxis.

---

9. Fünf Vorfälle, die das strukturelle Muster belegen

Fünf Vorfälle — drei aus 2026, zwei grundlegende ältere Fälle — veranschaulichen, warum zentralisierte Architekturen unter regulatorischem Druck versagen und warum dieses Versagen architektonischer und nicht operativer Natur ist.

9.1 Kaiser Foundation Health Plan — USD 47,5 Mio. Vergleich (2026)

Kaiser Foundation Health Plan schloss einen Sammelklage-Vergleich über USD 47,5 Millionen wegen Pixel-Tracking auf dem Patientenportal, mit endgültiger Genehmigung am 30. April 2026 (Class Action Center, Kaiser Foundation Health Plan-Vergleichsdossier). Die Kläger machten geltend, dass in Kaisers authentifiziertem Patientenportal eingebettete Meta- und Google-Tracking-Pixel geschützte Gesundheitsinformationen an Drittanbieter-Werbeplattformen übermittelt hätten — einschliesslich Diagnosen, Termintypen und Medikamentenanfragen — zusammen mit Kennungen, die ausreichten, um die Daten bestimmten Patienten zuzuordnen. Das architektonische Versagen ist präzise: Die Einwilligung der Patientinnen und Patienten existierte auf der Registrierungsebene des Portals, aber der Datenfluss wurde durch die eingebetteten SDKs bestimmt, nicht durch die erklärten Präferenzen der Patientinnen und Patienten. Das

Widerrufen der Einwilligung änderte nichts an den bereits übermittelten Pixelereignissen, und die Patientinnen und Patienten hatten keine architektonische Möglichkeit, die Drittanbieter-Datenflüsse zu erkennen oder zu unterbinden.

9.2 Sutter Health — USD 21,5 Mio. Vergleich (2026)

Sutter Health schloss einen Vergleich über USD 21,5 Millionen im gleichen Dossier-Muster, mit endgültiger Genehmigung am 27. Februar 2026. Parallele Vergleiche wurden gegen BJC HealthCare, Northwell Health, Catholic Health, Aspirus und SSM Health auf im Wesentlichen identischen Sachverhalten abgeschlossen oder sind hängig. Das gesamte Vergleichsdossier 2025–2026 ist der Frühindikator: Jedes grosse US-Gesundheitssystem, das Drittanbieter-Tracking-Pixel in patientenorientierten Oberflächen eingebettet hat, zahlt nun für das architektonische Fehlen pro-Patienten-kryptografischer Grenzen im Datenfluss. Die Einwilligung war ein Kästchen zum Abhaken; der Fluss wurde anderswo bestimmt.

9.3 NHS National Data Opt-Out (NDOO) — Nicht-Rückwirkung, 2018–2021

NHS England konsolidierte die bisherigen Opt-out-Typen 1 und 2 ab 2018 mit gesetzlicher Wirkung in den National Data Opt-Out (NDOO). Programmdokumentation und ICO-Kommentare bestätigten anschliessend, dass der Opt-out nachweislich **nicht rückwirkend** war: Daten, die bereits vor der Registrierung des Opt-out aus Hausarztpraxissystemen extrahiert worden waren, verblieben in Forschungsdatensätzen und konnten weiterhin verarbeitet werden. NHS Digital verfügte über keine technische Infrastruktur, um bereits extrahierte Datensätze zurückzurufen. Das Nachfolgeprogramm GPDPR (General Practice Data for Planning and Research) sollte am 1. Juli 2021 beginnen und wurde im Juni 2021 auf unbestimmte Zeit verschoben, da es keine technischen Mittel gab, bereits extrahierte Hausarztpraxisdaten zu löschen, wenn nachträglich ein Typ-1-Opt-out registriert wurde. Stand 2026 hat die Extraktion noch nicht begonnen. Die architektonische Lehre: Wenn der Betreiber den Datenpfad besitzt, hat das «Patientenveto» kein Durchsetzungsprimitiv — und der Policy-Mechanismus bricht unter seinem eigenen forensischen Gewicht zusammen.

9.4 SingHealth — 1,5 Millionen Datensätze kompromittiert (2018)

Der öffentliche Untersuchungsbericht des Singapore Committee of Inquiry zum Cyberangriff auf Singapore Health Services (10. Januar 2019) stellte fest, dass 1,5 Millionen SingHealth-Patientenakten kompromittiert worden waren, einschliesslich der persönlichen Krankenakte des Premierministers von Singapur. Der technische Befund ist der architektonische: Es gab **keine Kompartmentierung** im elektronischen Krankenaktensystem von SingHealth. Sobald ein Angreifer über ein privilegiertes Dienstkonto das Allscripts-Sunrise-System erreichte, waren alle Patientenakten zugänglich. Die Einwilligung der Patientinnen und Patienten war ein Policy-Artefakt auf der Zugriffsebene; die Datenschicht hatte **keine pro-Patient-kryptografische Grenze**. Die Angriffsfläche war genau das Fehlen dieser Grenze.

9.5 DigiNotar-Zertifizierungsstellenkompromittierung (2011)

Die Fox-IT-Untersuchung, veröffentlicht als «Black Tulip»-Bericht (13. August 2012), stellte fest, dass alle acht DigiNotar-CA-Server kompromittiert worden waren. Mehr als 531 betrügerische Zertifikate wurden ausgestellt, darunter ein Wildcard-Zertifikat `*.google.com`, das für einen Man-in-the-Middle-Angriff gegen rund 300.000 iranische Gmail-Nutzer eingesetzt wurde. Die Abhilfemassnahme — DigiNotar zu misstrauen — wurde von Mozilla, Microsoft und Google einseitig getroffen und über Root-Store-Updates an die Endnutzer weitergegeben. Die eigene Staat der Nederlanden–G2-Kette der niederländischen Regierung wurde bei der ersten Entfernung übersehen und erforderte Nacharbeit. Endnutzer hatten **keinerlei Handlungsmacht** bei der Vertrauensentscheidung in keiner Phase: nicht bei der Ausstellung, nicht bei der Erkennung, nicht bei der Behebung. Sie erfuhren von der Kompromittierung dadurch, dass ihre eigenen Dienste nicht mehr funktionierten.

Jeder zentralisierte Vorfall teilt ein Merkmal: Die Nutzenden hatten keine architektonische Handlungsmacht. Kaiser- und Sutter-Patienten kontrollierten den Pixel-Datenfluss nicht. NHS-Patienten konnten extrahierte Daten nicht zurückrufen. SingHealth-Patienten hatten keine pro-Datensatz-kryptografische Grenze. DigiNotar-Endnutzer konnten nicht über Vertrauensentscheidungen abstimmen. Das Muster ist strukturell und bleibt über fünf Jahrzehnte Vorfallbelege hinweg bestehen, unabhängig von Aufsichtsbehörde, Sektor oder Jurisdiction.

---

10. Fazit und nächste Schritte

Opt-out hat den Übergang von einer politischen Absichtserklärung zu einem durchsetzbaren gesetzlichen Recht vollzogen: unter EHDS Article 71, GDPR 7(3) und 17(2), eIDAS 2.0 5a(14)/(16)(b), dem Schweizer DSG und HFG sowie dem deutschen PDSG. Fünf technische Invarianten folgen daraus direkt: personenbezogene Kennungen, überprüfbarer zeitgestempelter Opt-out, Reversibilität ohne Re-Identifizierung, controllerübergreifende Weitergabe und Nicht-Verknüpfbarkeit. X.509 PKI erfüllt keine davon auf der Bürgerebene; föderiertes IAM erfüllt die Weitergabe-Invariante nur unter Verletzung der Nicht-Verknüpfbarkeit; zentralisiertes KMS erfüllt den Single-Tenant-Fall, kann jedoch keine Trust Domains überschreiten. **DKMS ist die erste strukturell tragfähige Grundlage, um Opt-out durchgängig zu wahren — in organisationsübergreifenden, nach der Offenlegung wirksamen, regulatorisch beaufsichtigten Konstellationen** — mit expliziten Grenzen bei Derivaten, Sicherungen und einzelnen unkooperativen Gegenparteien. Das Vergleichsdossier 2025–2026 (Kaiser, Sutter, BJC, Northwell, Catholic Health, Aspirus, SSM Health) ist der lebendige Beweis dafür, dass jede zentralisierte Architektur unter diesem regulatorischen Druck ein Merkmal teilt: Die Nutzenden hatten keine architektonische Handlungsmacht.

Wenn Sie für die Consent-Architektur in einem Gesundheits-IT-Bereich verantwortlich sind, der mit EHDS-Transposition, Schweizer EGDG/BDG-Implementierung oder deutschen PDSG-Abläufen konfrontiert ist, bietet Vereign einen 30-minütigen Consent-Architektur-Review an. Wir werden Ihre aktuelle Consent-Oberfläche gegen die fünf Invarianten abbilden, die Article 71(8)-Fallen in Ihrer Roadmap identifizieren und

den genauen Umfang bestimmen, in dem DKMS die richtige architektonische Antwort ist — und in dem es dies nicht ist. **Kontakt: contact@vereign.com.**

Vereign AG — Dammstrasse 16, 6300 Zug, Schweiz — UID CHE-240.299.384 — LEI 50670056G9BYC736YR76