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

Vereign AG

2026-04-29

Arquitetura de Consentimento: DKMS como Base Estruturalmente Sólida para o EHDS Article 71

Vereign AG — Abril de 2026

1. Sumário Executivo

O direito europeu em matéria de dados de saúde cruzou um limiar decisivo. O opt-out deixou de ser uma aspiração política — ao abrigo do EHDS Article 71, é um **direito legal** da pessoa singular, exequível em todos os Estados-Membros que tratam dados de saúde identificáveis para utilização secundária. Sobrepondo-se aos artigos GDPR Art 7(3) e 17(2), eIDAS 2.0 Article 5a, à FADP e HFG suíças e à PDSG alemã, cinco regimes independentes convergem num conjunto único de invariantes de engenharia: **identificadores com âmbito pessoal, opt-out verificável com carimbo temporal, reversibilidade sem re-identificação, propagação entre controladores e desvinculabilidade**. A PKI centralizada e a identidade federada satisfazem, no máximo, um ou dois desses requisitos; o X.509 não satisfaz nenhum ao nível do cidadão. **O Decentralized Key Management (DKMS) é a primeira base estruturalmente sólida para honrar a retirada do consentimento de ponta a ponta — *em condições inter-organizacionais, pós-divulgação e sob supervisão regulatória*.** A tese tem fronteiras explícitas: derivados que saíram do sistema antes da retirada, cópias de segurança imutáveis e contrapartes individualmente desonestas continuam fora do alcance arquitetural. O dossiê de acordos de 2025–2026 (Kaiser USD 47,5M, Sutter USD 21,5M, ações paralelas contra BJC, Northwell, Catholic Health, Aspirus

e SSM Health) é o indicador avançado: cada incidente centralizado partilha uma característica — o utilizador não tinha qualquer agência arquitetural.

---

2. Porquê Agora — Convergência Regulatória em 24 Meses

Durante duas décadas, a gestão de consentimento em TI de saúde tratou o opt-out como um problema de experiência do utilizador. A partir de 2024, cinco regimes jurídicos independentes convergiram no mesmo padrão de engenharia, deixando os fornecedores com meses — e não anos — para demonstrar conformidade estrutural.

EHDS Article 71 — Regulamento (UE) 2025/327. Adotado a 11 de fevereiro de 2025; publicado no Jornal Oficial da União Europeia (JO L 2025/327) a 5 de março de 2025; em vigor desde 26 de março de 2025. O artigo 71(1) confere a cada pessoa singular o direito de opt-out relativamente ao tratamento secundário de dados de saúde eletrónicos identificáveis. O artigo 71(2) proíbe a emissão de novas autorizações sobre dados identificáveis após o exercício do opt-out, preservando as autorizações emitidas antes desse exercício. **O Article 71(8)** proíbe os detentores de dados de adquirir dados de identificação adicionais unicamente para honrar o opt-out — o pivô de engenharia que inviabiliza o padrão óbvio de “registo central de IDs sujeitos a opt-out”.

GDPR Articles 7(3) e 17(2) — Regulamento (UE) 2016/679. O artigo 7(3) exige que a retirada do consentimento seja «tão fácil de retirar como de dar». O artigo 17(2) impõe um dever de propagação: um responsável pelo tratamento que honre um pedido de apagamento deve tomar «medidas razoáveis, incluindo medidas técnicas» para informar os responsáveis a jusante. O artigo 9(2)(a) eleva o limiar para os dados de saúde ao *consentimento explícito*; o artigo 17(3)(c)/(d) prevê exceções para a saúde pública e investigação que tornam o apagamento literal estruturalmente inatingível para a maioria dos registos clínicos — razão exata pela qual o EHDS formulou o direito como **supressão prospetiva** e não como eliminação retroativa.

eIDAS 2.0 — Regulamento (UE) 2024/1183. Altera o Regulamento (UE) 910/2014 para estabelecer a Carteira de Identidade Digital Europeia (EUDIW). O artigo 5a(14) exige «controlo total pelo utilizador» sobre as operações da carteira. O artigo 5a(16)(a) proíbe o rastreio inter-contextos da utilização da carteira; o artigo 5a(16)(b) exige a **desvinculabilidade** entre apresentações de credenciais a diferentes verificadores. Em conjunto, os artigos 5a(16)(a)–(b) constituem a forma operacional do EHDS Article 71(8): uma arquitetura em que o operador pode correlacionar um cidadão entre verificadores falha necessariamente no teste de desvinculabilidade.

FADP e HFG suíças. A Lei Federal sobre a Proteção de Dados revista (FADP / nDSG, SR 235.1, em vigor desde 1 de setembro de 2023) exige consentimento explícito para dados sensíveis no artigo 6(6) e um direito de retirada absoluto no artigo 6(7), com direitos de eliminação nos termos do artigo 32 sujeitos a obrigações de retenção. A Lei sobre a Investigação com Seres Humanos (HFG / HRA, SR 810.30) nos artigos 7(2) e 17 confere o direito de revogação do consentimento e um direito de oposição à utilização ulterior de dados de

saúde. O EGDG em preparação (mensagem do Conselho Federal, 5 de novembro de 2025) inverte o modelo do DSE de opt-in para opt-out com entrada em vigor prevista para ~2028–2030; o BDG (base jurídica para utilização secundária DigiSanté) encontra-se em fase de elaboração. A propagação inter-cantonal torna o caso suíço estruturalmente mais exigente do que o europeu.

PDSG alemã. O Patientendaten-Schutz-Gesetz operacionaliza a arquitetura de opt-out do ePA alemão (registo eletrónico do paciente), em operação desde janeiro de 2025, abrangendo aproximadamente 73 milhões de beneficiários do seguro de saúde obrigatório. A PDSG codifica as mecânicas de supressão prospetiva — os cidadãos que recusam o ePA não podem ser tratados ao abrigo da base jurídica de opt-in — para uma população maior do que a maioria dos Estados-Membros da UE combinados. A pressão de implementação nacional sobre a arquitetura de consentimento não é, portanto, teórica; é operacional no maior sistema de saúde de pagador único da Europa.

A orientação provisória da TEHDAS2 Joint Action (setembro de 2025) confirma que o mecanismo técnico de propagação do opt-out **não** é especificado pelo direito europeu em si, sendo delegado à implementação pelos Estados-Membros. Esta é a vulnerabilidade arquitetural: cada Estado pode escolher a sua abordagem, mas apenas uma abordagem de chaveamento controlado pelo sujeito satisfaz o Article 71(8) sem introduzir um registo de re-identificação proibido. Os fornecedores que apresentem uma arquitetura conforme num Estado-Membro venderão para todos os vinte e sete; os que resolverem apenas a experiência do utilizador local enfrentarão uma conversa arquitetural diferente em cada transposição.

Cada um destes cinco regimes, isoladamente, é ultrapassável. **Os cinco juntos, num intervalo de 24 meses, constituem a função de forçagem arquitetural.** Os fornecedores de TI de saúde deparam-se agora com um mercado em que a «gestão do consentimento» deve compor-se de ponta a ponta — entre fronteiras, entre controladores, ao longo do tempo — e o padrão de registo centralizado que sustentou a indústria durante duas décadas está inviabilizado pelo direito primário do maior bloco económico do planeta.

---

3. Os Cinco Invariantes de Engenharia

Os cinco regimes convergem num conjunto pequeno e preciso de requisitos de engenharia. Não são aspiracionais — são predicados testáveis com os quais qualquer arquitetura de consentimento pode ser avaliada.

3.1 Identificadores com Âmbito Pessoal

O titular dos dados deve controlar o identificador sob o qual as suas autorizações e o seu estado de consentimento são referenciados. Este é o *pré-requisito* para todos os outros invariantes: se o operador detém o identificador, detém o opt-out. O EHDS Article 71(8) inviabiliza explicitamente os registos de re-identificação do lado do operador; o mandato de «controlo total pelo utilizador» do eIDAS 2.0 Article 5a(14) nomeia a mesma propriedade ao nível da carteira. Sem um identificador com âmbito no sujeito, a propagação, a reversibilidade e a desvinculabilidade colapsam em política do operador.

3.2 Opt-Out Verificável com Carimbo Temporal

Para cada autorização de dados, o sistema deve conhecer o momento preciso da emissão e o momento preciso da retirada — e um terceiro (regulador, tribunal, controlador a jusante) deve poder verificar ambos sem ter de confiar nos registos do operador. O EHDS Article 71(2) estabelece uma fronteira temporal nítida: as autorizações anteriores ao opt-out permanecem válidas; as posteriores são ilegais. Isto é inexequível sem uma linha do tempo à prova de adulteração e verificável por terceiros do estado de consentimento do sujeito.

3.3 Reversibilidade sem Re-Identificação

O Recital 54 do Regulamento EHDS confirma que o opt-out é reversível (os cidadãos podem optar por voltar a incluir-se) e de forma livre (sem duração mínima). O Article 71(8) proíbe o detentor de dados de adquirir dados de identificação adicionais unicamente para honrar o opt-out. As duas cláusulas lidas em conjunto criam uma restrição apertada: o sistema deve suportar a alternância do estado de consentimento ao ritmo do cidadão, **sem** que o detentor de dados construa um registo paralelo de re-identificação para rastrear quem alterou em que sentido. Qualquer arquitetura que exija «manter uma lista de IDs sujeitos a opt-out» viola o artigo 71(8) diretamente.

3.4 Propagação entre Controladores

O GDPR Article 17(2) exige que o responsável pelo tratamento que honre o apagamento tome «medidas razoáveis, incluindo medidas técnicas» para informar os controladores a jusante que detêm cópias, replicações ou ligações. O EHDS Article 71 sobreposto a cadeias de autorizações multi-controlador agrava isto: o sinal de opt-out deve chegar a cada Organismo de Acesso a Dados de Saúde, a cada consórcio de investigação, a cada subprocessador que recebeu dados ao abrigo de uma autorização anterior. A propagação não pode ser um registo em papel — tem de ser um artefacto verificável que as partes a jusante possam reverificar.

3.5 Desvinculabilidade

O eIDAS 2.0 Article 5a(16)(b) exige a desvinculabilidade entre apresentações da mesma credencial a diferentes verificadores. A consequência operacional: uma arquitetura em que qualquer parte singular (mesmo um intermediário autorizado) vê todas as transações entre verificadores falha o teste por construção. Esta é a propriedade que exclui os fornecedores de identidade federada da camada do cidadão em sistemas conformes com o EHDS: o IdP, por conceção, vê cada autenticação e cada apresentação de credencial. A federação pode satisfazer a propagação, mas apenas violando a desvinculabilidade.

Estes cinco invariantes formam um sistema interligado. **O X.509 PKI não satisfaz nenhum ao nível do cidadão. Os IdPs federados satisfazem a propagação apenas violando a desvinculabilidade. O DKMS satisfaz todos os cinco.** Esta é a afirmação de solidez estrutural, e o restante deste documento examina-a em detalhe.

---

4. A Armadilha do Article 71(8)

O padrão de implementação mais simples para o opt-out — aquele que um fornecedor de TI de saúde rascunharia na primeira hora de conversa arquitetural — é **um registo central de IDs de cidadãos sujeitos a opt-out**. Cada detentor de dados consulta o registo antes do tratamento; se o ID do cidadão constar da lista, o tratamento é interrompido. Simples. Familiar. Auditável.

O Article 71(8) inviabiliza completamente este padrão.

A cláusula proíbe os detentores de dados de adquirir dados de identificação adicionais unicamente para honrar o opt-out. **A «lista de IDs sujeitos a opt-out» é, por construção, exatamente esse registo.** Existe apenas com o propósito de re-identificar cidadãos para o caso negativo — para determinar que *este cidadão tem opt-out ativo e portanto não pode ser tratado*. A própria lista constitui a violação regulatória que visa prevenir.

A armadilha é recursiva. Qualquer tentativa de anonimizar o registo (aplicar hash aos IDs, pseudonimizá-los, mantê-los num domínio de confiança separado) reintroduz o problema original: o detentor de dados continua a precisar de *algum* identificador para testar contra a lista, e esse identificador tem de ser derivável dos dados que o detentor já possui. O hash não é anónimo para o detentor que tem o input; o pseudónimo não é anónimo para o detentor que tem a ligação. O Recital 54 reforça isto ao exigir que o opt-out seja reversível e de forma livre — o que significa que o registo deve suportar alternância, o que por sua vez exige que o registo rastreie *qual* cidadão alterou *quando*, que é precisamente o registo de re-identificação que o artigo 71(8) proíbe.

A implicação para os fornecedores de TI de saúde é clara. **Qualquer «módulo de gestão de consentimento» cuja arquitetura assente numa lista central autoritária de sujeitos com opt-out ativo está inviabilizado pelo direito primário da UE.** Esta não é uma escolha de design de experiência do utilizador; é a diferença entre uma arquitetura que pode cumprir o EHDS e uma que não pode. Os produtos genéricos de gestão de consentimento assentes no padrão de registo — sejam SaaS, on-prem ou híbridos — enfrentarão esta restrição em cada transposição de Estado-Membro. A resposta estrutural deve colocar o identificador sob controlo do cidadão, de modo que o detentor de dados nunca precise de manter um registo de re-identificação.

---

5. A Tese DKMS

> **O Decentralized Key Management é a primeira base estruturalmente sólida para honrar a retirada do consentimento de ponta a ponta — *em condições inter-organizacionais, pós-divulgação e sob supervisão regulatória*.**

O DKMS — assente no KERI, uma especificação aberta da Trust over IP Foundation — coloca a raiz de confiança no cidadão em vez de numa autoridade centralizada. O cidadão (ou o seu agente de carteira) detém um Autonomic IDentifier (AID) que é auto-certificável: é derivado de uma chave pública sob controlo do cidadão, e a sua autenticidade não depende de nenhum registador. Todas as autorizações concedidas a

detentores de dados, processadores e controladores a jusante encadeiam-se nesse AID através de um Key Event Log (KEL) — um registo de apenas adição, verificável por terceiros, do estado de chaveamento do cidadão, incluindo rotações de chaves.

A retirada neste modelo não é um pedido submetido a um operador. É uma **rotação de chave que o cidadão realiza unilateralmente**. A rotação é publicada no KEL; a partir desse momento, qualquer parte a jusante que detenha credenciais ancoradas ao estado de chave pré-rotação deve re-autenticar-se face ao estado atual do cidadão para continuar o tratamento. As autorizações existentes emitidas antes da rotação continuam a operar onde a base jurídica subjacente o permite (correspondendo ao EHDS Article 71(2)); novas autorizações não podem ser emitidas sob o antigo estado de chave, porque esse estado já não é o estado controlador do cidadão. O cidadão retirou arquiteturalmente — e não apenas procedimentalmente — a autorização futura, e qualquer parte a jusante que ignore a rotação publicada produz assinaturas auditáveis como desatualizadas.

Mapeando isto face aos cinco invariantes:

Invariante	**Mecanismo DKMS**
Identificadores com âmbito pessoal	O AID é o identificador auto-certificável do sujeito; não é necessário nenhum índice do lado do operador
Opt-out verificável com carimbo temporal	O KEL contém eventos de chave com carimbo temporal à prova de adulteração
Reversibilidade sem re-identificação	Opt-back-in = rotação de chave que restabelece a autorização; sem registo paralelo
Propagação entre controladores	O KEL é publicável; os verificadores devem reverificar entre domínios de confiança
Desvinculabilidade	AIDs por contexto e credenciais com divulgação seletiva evitam a correlação entre verificadores

Comparando com as opções existentes:

X.509 PKI vincula a identidade a um certificado emitido por uma Autoridade de Certificação. O cidadão não detém a raiz de confiança; a CA detém-na. A revogação é conduzida pelo operador (CRL/OCSP) e falha silenciosamente por omissão. A desvinculabilidade inter-contextos é estruturalmente ausente — cada apresentação de certificado é vinculável através do número de série do certificado, DN do emissor e DN do sujeito. O X.509 não satisfaz *nenhum* dos cinco invariantes ao nível do cidadão.

IAM Federado (OIDC, SAML). O Identity Provider é, por conceção, o rastreador inter-contextos que o eIDAS 2.0 Article 5a(16)(b) proíbe. A federação pode satisfazer a propagação entre controladores (um single logout encerra sessões a jusante), mas apenas violando a desvinculabilidade — cada autenticação passa pelo IdP, que vê cada parte confiante que o cidadão visita. A arquitetura pode satisfazer no máximo três invariantes e apenas ao custo do quinto.

KMS Centralizado (AWS KMS, Azure Key Vault, GCP Cloud KMS). Excelente para cargas de trabalho de inquilino único. O apagamento criptográfico NIST SP 800-88 §2.5 via Customer-Managed Keys é uma primitiva de apagamento terminal reconhecida pelos reguladores (EDPB Guidelines 01/2025; ENISA 2019

§4.2). Mas assim que os dados saem do perímetro do inquilino — para um consórcio de investigação, um controlador a jusante, um destinatário de utilização secundária permitida — a destruição da CMK do operador não tem qualquer efeito sobre a cópia. A propagação entre controladores permanece não resolvida. Schrems II / EDPB Recommendations 01/2020 Use Case 3 agrava ainda mais isto: o importador de dados não deve deter as chaves, por definição.

O DKMS não substitui estas pilhas — ocupa o slot arquitetural preciso que elas não conseguem preencher. KMS centralizado para apagamento com âmbito no inquilino, X.509 para revogação ao nível de TLS, IAM federado para consentimento com âmbito de sessão — e DKMS para a camada inter-organizacional, pós-divulgação, onde o EHDS Article 71 realmente existe.

---

6. Onde as Arquiteturas Centralizadas Falham

Os cinco invariantes são testáveis. Cada grande arquitetura centralizada de consentimento falha de forma estruturalmente específica.

6.1 O X.509 PKI Falha em Todos os Cinco Invariantes ao Nível do Cidadão

O X.509 vincula a identidade a uma Autoridade de Certificação. A CA gera ou co-assina o certificado do cidadão, detém a decisão de emissão e controla a revogação. Os identificadores com âmbito pessoal falham na raiz — a assinatura da CA é a fonte de confiança, não a do cidadão. O opt-out com carimbo temporal é conduzido pelo operador (o cidadão submete um pedido de revogação; a CA decide se o honra e quando o publica), e a revogação propaga-se apenas à velocidade das janelas de atualização das CRL ou da disponibilidade do respondedor OCSP — ambos os quais falham silenciosamente nos navegadores por omissão. A reversibilidade sem re-identificação falha porque a re-emissão exige que a CA re-valide a identidade do sujeito, o que em contextos de saúde exige que a CA re-adquira os mesmos dados de identificação que o EHDS Article 71(8) proíbe o detentor de dados de deter. A propagação entre controladores depende de cada parte confiante verificar corretamente as CRL/OCSP, o que os incidentes DigiNotar e Comodo demonstraram ser operacionalmente frágil. A desvinculabilidade é estruturalmente impossível: cada certificado X.509 transporta um número de série e um DN do emissor que ligam cada apresentação ao mesmo cidadão.

6.2 O IAM Federado (OIDC/SAML) Falha na Desvinculabilidade por Definição

O OIDC e o SAML federam a autenticação através de um Identity Provider que intermedeia a relação entre o cidadão e a parte confiante. Cada autenticação que o cidadão realiza face a qualquer verificador passa pelo IdP. O IdP sabe qual cidadão acedeu a qual serviço quando. Esta não é uma escolha de configuração ou uma violação de política — é a função arquitetural do IdP. O eIDAS 2.0 Article 5a(16)(b) exige a desvinculabilidade entre apresentações da mesma credencial a diferentes verificadores; o IdP federado é, por construção, o ponto singular onde cada apresentação é correlacionada. A federação pode proporcionar propagação real entre

controladores (Single Logout, OAuth Token Revocation, OIDC Back-Channel Logout) — mas o custo é a violação do invariante de desvinculabilidade para cada apresentação de credencial que o IdP intermedeia.

6.3 O KMS Centralizado Não Consegue Alcançar a Propagação entre Controladores

O AWS KMS, o Azure Key Vault e o GCP Cloud KMS proporcionam custódia de chaves auditável, backends FIPS 140-2 L3 / 140-3, destruição programada de chaves (`ScheduleKeyDeletion`, soft-delete + purge, `DESTROY_SCHEDULED`) e cifragem em envelope com separação DEK/KEK. Dentro de um único inquilino, esta é uma primitiva de apagamento GDPR Article 17 plenamente adequada — o NIST SP 800-88 §2.5 reconhece explicitamente o Apagamento Criptográfico como uma técnica de sanitização ao nível Purge, e as EDPB Guidelines 01/2025 tratam a custódia de chaves como determinante do resultado para efeitos de saber se os dados são anónimos para um determinado destinatário. A arquitetura funciona **dentro do perímetro do inquilino**.

Não cruza esse perímetro. Assim que os dados foram copiados legalmente para um consórcio de investigação, um controlador a jusante autorizado ou um subprocessador noutro domínio de confiança, a destruição do KMS do inquilino não tem qualquer efeito sobre a cópia. A propagação ao abrigo do GDPR Article 17(2) torna-se uma obrigação contratual — documentação em papel, não arquitetura. A estrutura de cadeias de autorizações do EHDS Article 71 torna esta lacuna estrutural em vez de incidental: cada autorização é potencialmente o início de uma cadeia multi-controlador, e a CMK centralizada não tem meios de alcançar além do primeiro elo.

---

7. Onde o DKMS NÃO Entrega — Análise Rigorosa dos Limites

A tese é estrutural, não absoluta. Um enquadramento honesto torna o argumento defensável; o excesso destrói-o. A afirmação DKMS tem quatro fronteiras explícitas.

7.1 Derivados — EDPB Opinion 28/2024

Assim que os dados foram transformados num derivado — agregados analíticos, pesos de modelos de ML, extratos estatísticos, relatórios regulatórios já arquivados — a destruição de chaves no texto cifrado de origem não tem qualquer efeito sobre o derivado. A EDPB Opinion 28/2024 sobre aspetos de proteção de dados em modelos de IA (adotada a 17 de dezembro de 2024) confirma explicitamente que as obrigações de apagamento não se propagam de forma limpa para os pesos de modelos depois de o treino ter ocorrido. O DKMS não é melhor do que a CMK centralizada neste caso. Se um consórcio de investigação autorizado treinou um modelo com dados de um cidadão que posteriormente exerce o opt-out, os pesos do modelo permanecem. A contribuição arquitetural é a auditabilidade da cadeia de derivação, não o desfazer retroativo da derivação.

7.2 Cópias de Segurança Já Efetuadas

Nenhuma arquitetura de revogação de chaves ativas — DKMS ou centralizada — pode recolher dados já replicados em suportes de cópia de segurança imutáveis. As cópias de segurança offline efetuadas antes da retirada situam-se fora do espaço de chaves ativas. A resposta pragmática é a destruição programada e documentada de chaves numa janela de retenção conhecida — que as orientações do ICO, CNIL e BfDI reconhecem como suficiente para dados pessoais residuais em cópias de segurança. O DKMS alinha-se com esta disciplina; não a substitui.

7.3 Contraparte Individualmente Desonesta

Numa rede de N partes com uma parte que ignora a rotação de chave publicada e continua a agir com base em credenciais desatualizadas, o DKMS proporciona **deteção forense** — as assinaturas desatualizadas são auditáveis após o evento de rotação publicado — mas não **prevenção**. Um processador a jusante totalmente não cooperante que exfiltra texto em claro e o armazena fora do envelope chaveado não está ao alcance arquitetural de nenhum sistema de gestão de chaves. O DKMS reforça a posição probatória do regulador; não elimina a necessidade de contrato, regulador ou tribunal para agir contra atores de má-fé. Comparado com um parque de CMK centralizado bem governado contratualmente, o DKMS reforça a deteção mas não elimina a necessidade de execução contra atores de má-fé.

7.4 Cargas de Trabalho de Inquilino Único

Para cargas de trabalho que vivem inteiramente dentro de um domínio de confiança — dados empresariais internos sob um único controlador, SaaS de inquilino único com CMK com âmbito no inquilino, TLS de web pública ao abrigo dos SLOs de revogação de 24 horas do CA/Browser Forum — o apagamento criptográfico NIST SP 800-88 §2.5 via CMK centralizada é plenamente adequado. As EDPB Guidelines 01/2025 e a ENISA 2019 §4.2 reconhecem a destruição de chaves como apagamento terminal dentro do perímetro do inquilino. **Adicionar DKMS a estas cargas de trabalho impõe encargos operacionais sem qualquer benefício arquitetural.** A resposta honesta é que, para cenários de inquilino único, a pilha centralizada funciona.

7.5 A Fronteira Decisiva

O DKMS domina quando se verificam **todas as quatro** condições seguintes:

1. Os dados cruzam **pelo menos dois domínios de confiança**.
2. O consentimento deve **sobreviver pós-divulgação** (ou seja, o tratamento continua além do perímetro).
3. O regulador trata a **custódia de chaves como determinante do resultado** (Schrems II / EDPB Recommendations 01/2020 Use Case 3 / EHDS Article 71(8)).
4. As partes compõem o DKMS **de ponta a ponta** (um verificador que ignora o KEL anula a cadeia).

Fora dessas quatro condições, a CMK centralizada é a escolha racional, e dizê-lo torna a tese DKMS mais forte — e não mais fraca — porque localiza a afirmação precisamente onde as evidências a sustentam. A afirmação não é que o DKMS resolve banners de cookies ou a eliminação em SaaS de inquilino único. A afirmação é que

o DKMS é a escolha estrutural correta para *exatamente* os casos que importam para o consentimento em saúde inter-cantonal, inter-organizacional, sob supervisão regulatória e pós-divulgação.

---

8. Prova em Produção

A Vereign opera a arquitetura DKMS em produção atualmente, com ressalvas explícitas sobre o que está em produção versus o que é arquitetural.

SEAL é a camada de comunicação em produção: entrega em enxame cifrado para comunicação de saída, com chaves por mensagem e agência de desencriptação controlada pelo destinatário. O SEAL tem transportado **mais de 800.000 mensagens verificadas por mês** para utilizadores institucionais — o ponto de ancoragem de produção à escala para a arquitetura. Cada mensagem exercita o mesmo substrato de eventos de chave que subjaz à tese de consentimento: chaveamento controlado pelo sujeito, carimbos temporais verificáveis por terceiros e desvinculabilidade por contexto entre destinatários.

Stargate — a camada de autorização ancorada em AID onde as autorizações de dados se encadeiam no KEL do cidadão — entra em produção inicial a partir de junho de 2026 com a HIN como primeiro desdobramento operacional. O Stargate é a superfície de consentimento da tese: as autorizações concedidas aos detentores de dados estão ancoradas no AID do cidadão; a rotação de chave pelo cidadão propaga-se através do KEL; os verificadores a jusante reverificam. O desdobramento HIN é um lançamento suave em termos de âmbito; **o discurso de adoção em massa está reservado para depois do verão de 2026**, após o coorte de produção inicial ter acumulado evidências operacionais em condições regulatórias reais.

As pontes HIN permitem que a retirada interopere com contrapartes que utilizam X.509, através da ponte S/MIME ancorada em KERI documentada na base de conhecimento de segurança de e-mail. Este é o reconhecimento pragmático de que o DKMS irá compor com — e não substituir de um dia para o outro — o parque X.509 de saúde existente.

FHIR-over-Stargate é hoje arquitetural — a implantação em produção depende do onboarding do lado hospitalar; a data mais realista é setembro de 2026. A narrativa arquitetural é genuinamente sólida: os recursos FHIR que fluem através do Stargate herdam o modelo de autorização ancorado em AID, pelo que o estado de consentimento ao nível do recurso existe onde o cidadão o controla. Mas a engenharia da adoção hospitalar — integração com sistemas clínicos, aprovação regulatória, governação operacional — é um empreendimento de múltiplos trimestres. Não afirmamos o FHIR-over-Stargate como já implementado. Afirmamo-lo como o próximo passo deliberado, com uma data mais cedo conhecida, e esperamos que a implantação operacional fique atrás da prontidão arquitetural por um intervalo mensurável. Confundir os dois é o modo de falha que este documento foi escrito para evitar.

O historial de produção importa porque é o que separa esta tese de uma apresentação de diapositivos. As organizações de engenharia encontram o argumento centralização versus descentralização com frequência; o que raramente encontram é a descentralização a operar à escala, sob regulação institucional real, numa indústria regulada. O substrato de mensagens verificadas tem transportado tráfego institucional real por tempo suficiente

para expor os casos limite operacionais do DKMS — disciplina de rotação de chaves, descoberta inter-organizacional, retenção de registos de auditoria, agência do destinatário — e esses casos limite foram refinados em produção e não na teoria. Quando o Stargate entra em produção inicial a partir de junho de 2026, funcionará no mesmo substrato. O argumento arquitetural não é, portanto, uma previsão; é uma extrapolação a partir de operações observadas à escala.

---

9. Cinco Incidentes que Comprovam o Padrão Estrutural

Cinco incidentes — três de 2026, dois casos fundamentais mais antigos — ilustram por que razão as arquiteturas centralizadas falham sob pressão regulatória e como o modo de falha é arquitetural em vez de operacional.

9.1 Kaiser Foundation Health Plan — Acordo de USD 47,5M (2026)

A Kaiser Foundation Health Plan chegou a um acordo de ação coletiva de USD 47,5 milhões sobre o rastreio por pixel no portal do paciente, com aprovação final a 30 de abril de 2026 (Class Action Center, dossiê de acordo Kaiser Foundation Health Plan). Os demandantes alegaram que pixels de rastreio da Meta e Google incorporados no portal autenticado de pacientes da Kaiser transmitiram informações de saúde protegidas a plataformas de publicidade de terceiros — incluindo diagnósticos, tipos de consultas e pesquisas de medicamentos — juntamente com identificadores suficientes para re-ligar os dados a pacientes específicos. A falha arquitetural é precisa: o consentimento do paciente existia na camada de registo do portal, mas o fluxo de dados era determinado pelos SDKs incorporados, não pela preferência declarada pelo paciente. A retirada do consentimento não tinha qualquer efeito sobre os eventos de pixel já transmitidos, e o paciente não tinha meios arquiteturais para detetar ou revogar os fluxos para terceiros.

9.2 Sutter Health — Acordo de USD 21,5M (2026)

A Sutter Health chegou a um acordo de USD 21,5 milhões no mesmo padrão de dossiê, com aprovação final a 27 de fevereiro de 2026. Acordos paralelos foram celebrados ou estão pendentes contra a BJC HealthCare, Northwell Health, Catholic Health, Aspirus e SSM Health em factos essencialmente idênticos. O dossiê de acordos de 2025–2026 no seu conjunto é o indicador avançado: cada grande sistema de saúde dos EUA que incorporou pixels de rastreio de terceiros em superfícies voltadas para pacientes está agora a pagar pela ausência arquitetural de fronteiras criptográficas por paciente no fluxo de dados. O consentimento era uma caixa de verificação; o fluxo era decidido noutro lugar.

9.3 NHS National Data Opt-Out (NDOO) — Não Retroatividade, 2018–2021

O NHS England consolidou os opt-outs de Tipo 1 e Tipo 2 legados no National Data Opt-Out (NDOO) a partir de 2018, com força estatutária. A documentação do programa e os comentários do ICO confirmaram subsequentemente que o opt-out era demonstravelmente **não retroativo**: os dados já extraídos dos sistemas de medicina geral antes de o cidadão registar o opt-out permaneciam nos conjuntos de dados de investigação e podiam continuar a ser tratados. O NHS Digital não tinha infraestrutura técnica para recuperar registos já extraídos. O programa sucessor GPDPR (General Practice Data for Planning and Research) estava programado para começar a 1 de julho de 2021 e foi adiado indefinidamente em junho de 2021 especificamente porque não havia meios técnicos para apagar dados de medicina geral já extraídos quando um opt-out de Tipo 1 era registado a posteriori. A extração ainda não começou em 2026. A lição arquitetural: quando o operador detém o caminho dos dados, o «veto do paciente» não tem primitiva de execução — e o mecanismo de política colapsa sob o seu próprio peso forense.

9.4 SingHealth — 1,5M de Registos Comprometidos (2018)

O Relatório Público do Comité de Inquérito de Singapura sobre o Ciberataque aos Serviços de Saúde de Singapura (10 de janeiro de 2019) concluiu que 1,5 milhões de registos de pacientes do SingHealth tinham sido comprometidos, incluindo o registo de saúde pessoal do Primeiro-Ministro de Singapura. A conclusão técnica é a arquitetural: não havia **compartimentação** no sistema de registos médicos eletrónicos do SingHealth. Assim que um atacante alcançou a aplicação Allscripts Sunrise através de uma conta de serviço privilegiada, todos os registos de pacientes estavam acessíveis. O consentimento do paciente era um artefacto de política na camada de acesso; a camada de dados não tinha **fronteira criptográfica por paciente**. A superfície de ataque era precisamente a ausência dessa fronteira.

9.5 Comprometimento da Autoridade de Certificação DigiNotar (2011)

A investigação da Fox-IT publicada como o relatório «Black Tulip» (13 de agosto de 2012) concluiu que todos os oito servidores CA da DigiNotar tinham sido comprometidos. Mais de 531 certificados fraudulentos tinham sido emitidos, incluindo um certificado wildcard `*.google.com` utilizado para montar um ataque man-in-the-middle contra aproximadamente 300.000 utilizadores iranianos do Gmail. A remediação — desconfiar da DigiNotar — foi tomada unilateralmente pela Mozilla, Microsoft e Google e propagada aos utilizadores finais através de atualizações ao repositório de certificados raiz. A própria cadeia Staat der Nederlanden – G2 do governo holandês foi ignorada na remoção inicial e exigiu seguimento. Os utilizadores finais não tinham **qualquer agência** na decisão de confiança em nenhuma fase: nem na emissão, nem na deteção, nem na remediação. Souberam do comprometimento através dos seus próprios serviços a falhar.

Cada incidente centralizado partilha uma característica: o utilizador não tinha agência arquitetural. Os pacientes da Kaiser e da Sutter não controlavam o fluxo de pixels. Os pacientes do NHS não conseguiam recuperar dados extraídos. Os pacientes do SingHealth não tinham fronteira criptográfica por registo. Os

utilizadores finais da DigiNotar não podiam votar nas decisões de confiança. O padrão é estrutural, e persiste ao longo de cinco décadas de evidências de incidentes, independentemente do regulador, setor ou jurisdição.

---

10. Conclusão e Como Envolver-se

O opt-out passou de aspiração política a direito legal exequível ao abrigo do EHDS Article 71, GDPR 7(3) e 17(2), eIDAS 2.0 5a(14)/(16)(b), FADP e HFG suíças e PDSG alemã. Cinco invariantes de engenharia decorrem diretamente: identificadores com âmbito pessoal, opt-out verificável com carimbo temporal, reversibilidade sem re-identificação, propagação entre controladores e desvinculabilidade. O X.509 PKI não satisfaz nenhum ao nível do cidadão; o IAM federado satisfaz a propagação apenas violando a desvinculabilidade; o KMS centralizado satisfaz o caso de inquilino único mas não consegue alcançar entre domínios de confiança. **O DKMS é a primeira base estruturalmente sólida para honrar a retirada do consentimento de ponta a ponta em condições inter-organizacionais, pós-divulgação e sob supervisão regulatória** — com fronteiras explícitas em torno de derivados, cópias de segurança e contrapartes individualmente desonestas. O dossiê de acordos de 2025–2026 (Kaiser, Sutter, BJC, Northwell, Catholic Health, Aspirus, SSM Health) é a evidência em tempo real de que cada arquitetura centralizada sob este tipo de pressão regulatória partilha uma característica: o utilizador não tinha agência arquitetural.

Se é responsável pela arquitetura de consentimento num parque de TI de saúde que enfrenta a transposição do EHDS, a implementação suíça do EGDG / BDG ou as operações PDSG alemãs, a Vereign oferece uma revisão de 30 minutos da arquitetura de consentimento. Mapearemos a sua superfície de consentimento atual face aos cinco invariantes, identificaremos as armadilhas do Article 71(8) no seu roteiro e localizaremos o âmbito preciso onde o DKMS é — e não é — a resposta arquitetural correta. **Contacto: contact@vereign.com.**

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