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

Vereign AG

2026-04-29

Архитектура на съгласието: DKMS като структурно стабилна основа за EHDS Article 71

Vereign AG — Април 2026 г.

1. Резюме

Европейското законодателство в областта на здравните данни е достигнало нова граница. Opt-out вече не е политическа декларация — съгласно EHDS Article 71 това е **законово право** на физическото лице, приложимо в всяка държава членка, която обработва идентифицируеми здравни данни за вторични цели. Наслоен върху GDPR Articles 7(3) и 17(2), eIDAS 2.0 Article 5a, швейцарските FADP и HFG и германския PDSG, пет независими правни режима се събират около един и същ набор от инженерни инварианти: **идентификатори, обвързани с личността, проверим opt-out с времеви печат, обратимост без повторна идентификация, разпространение между администратори и липса на свързаност**. Централизираният PKI и федерираната идентичност покриват в най-добрия случай един или два от тях; X.509 не покрива нито един на гражданско ниво. **Децентрализираното управление на ключове (DKMS) е първата структурно стабилна основа за зачитане на opt-out от край до край — *в условия на междуорганизационен поток, след-разкриване и регулаторно наблюдение*.** Тезата има ясни граници — производни данни, напуснали системата преди оттеглянето, неизменяеми архиви и единичен недобросъвестен контрагент остават извън архитектурния обхват. Списъкът на спогодбите за

2025–2026 г. (Kaiser — 47,5 млн. USD, Sutter — 21,5 млн. USD, паралелни производства срещу BJC, Northwell, Catholic Health, Aspirus и SSM Health) е водещият индикатор: при всеки централизиран инцидент е налице един общ белег — потребителят не е имал архитектурна свобода на действие.

---

2. Защо сега — регулаторна конвергенция в рамките на 24 месеца

В продължение на две десетилетия управлението на съгласието в здравната IT индустрия третираше opt-out като UX проблем. От 2024 г. насам пет независими правни режима се насочиха към един и същ инженерен модел, оставяйки на доставчиците месеци — не години — за да демонстрират структурно съответствие.

EHDS Article 71 — Reg. (EU) 2025/327. Прието на 11 февруари 2025 г.; публикувано в Официален вестник на Европейския съюз (OJ L 2025/327) на 5 март 2025 г.; в сила от 26 март 2025 г. Article 71(1) дава на всяко физическо лице правото да упражни opt-out от вторичното обработване на идентифицируеми електронни здравни данни. Article 71(2) забранява издаването на нови разрешения за обработване на идентифицируеми данни след упражняването на opt-out, като запазва валидността на разрешенията, издадени преди него. **Article 71(8)** забранява на притежателите на данни да придобиват допълнителни идентификационни данни единствено с цел изпълнение на opt-out — инженерната ос, която изключва очевидния модел с „централен регистър на гражданите, упражнили opt-out”.

GDPR Articles 7(3) и 17(2) — Reg. (EU) 2016/679. Article 7(3) изисква оттеглянето на съгласие да бъде „толкова лесно, колкото и даването му”. Article 17(2) въвежда задължение за разпространение: администратор, изпълняващ искане за заличаване, трябва да предприеме „разумни стъпки, включително технически мерки”, за да уведоми последващите администратори. Article 9(2)(a) повишава прага за здравните данни до *изрично* съгласие; Article 17(3)(c)/(d) предвижда изключения за обществено здраве и научни изследвания, поради което буквалното заличаване е структурно непостижимо за повечето клинични записи — именно затова EHDS формулира правото като **предстоящо потискане**, а не ретроактивно заличаване.

eIDAS 2.0 — Reg. (EU) 2024/1183. Изменя Reg. (EU) 910/2014 и въвежда Европейски портфейл за цифрова самоличност (EUDIW). Article 5a(14) изисква „пълен потребителски контрол” върху операциите с портфейла. Article 5a(16)(a) забранява проследяването между различни контексти на употреба на портфейла; Article 5a(16)(b) изисква **липса на свързаност** между представянията на идентификационни данни пред различни проверяващи. Заедно, 5a(16)(a)–(b) са оперативната форма на EHDS Article 71(8): архитектура, при която операторът може да корелира гражданина между различни проверяващи, не отговаря по дефиниция на изискването за липса на свързаност.

Швейцарски FADP и HFG. Ревизираният Федерален закон за защита на данните (FADP / nDSG, SR 235.1, в сила от 1 септември 2023 г.) изисква изрично съгласие за чувствителни данни съгласно Article 6(6) и абсолютно право на оттегляне съгласно Article 6(7), като правата на заличаване по Article 32 са

предмет на задължения за съхранение. Законът за научни изследвания с хора (HFG / HRA, SR 810.30) по Article 7(2) и Article 17 предоставя право на отмяна на съгласието и право на несъгласие за по-нататъшно използване на здравни данни. Предстоящият EGDG (послание на федералния съвет, 5 ноември 2025 г.) обръща модела на EPD от opt-in към opt-out с предвидено влизане в сила ~2028–2030 г.; BDG (правно основание за вторично използване по DigiSanté) е в процес на изготвяне. Междукантоналното разпространение прави швейцарският случай структурно по-сложен от европейския.

Германски PDSG. Законът за защита на данните на пациентите (Patientendaten-Schutz-Gesetz) прилага opt-out архитектурата на германската ePA (електронна пациентска карта), която е в production от януари 2025 г. при около 73 милиона осигурени лица в задължителната система. PDSG кодифицира механиката на предстоящото потискане — граждани, отказали ePA, не могат да бъдат обработвани въз основа на opt-in правното основание — при население, по-голямо от повечето държави членки на ЕС взети поотделно. Националният натиск за изпълнение на изискванията към архитектурата на съгласието вече не е теоретичен; той е операционен в най-голямата система с единствен платец в Европа.

Проектонасоките на Съвместно действие TEHDAS2 (септември 2025 г.) потвърждават, че техническият механизъм за разпространение на opt-out **не е** уреден от самото право на ЕС и е оставен на изпълнение на държавите членки. Това е архитектурната слаба точка: всяка държава може да избере собствен подход, но само подход с ключове, контролирани от субекта, отговаря на Article 71(8), без да въвежда забранен регистър за повторна идентификация. Доставчиците, които предложат отговаряща на изискванията архитектура в една държава членка, ще я продадат в двадесет и седемте; тези, които решат само локалния UX проблем, ще се изправят пред различен архитектурен разговор при всяка транспозиция.

Всеки от тези пет режима поотделно може да бъде преодолян. **Всичките пет заедно, в рамките на 24 месеца, са архитектурната принудителна функция.** Доставчиците на здравна IT сега са изправени пред пазар, в който „управлението на съгласието" трябва да работи end-to-end, презгранично, между администратори, в течение на времето — и моделът на централизирания регистър, поддържал индустрията в продължение на две десетилетия, е изключен от основното право на най-голямото икономическо пространство в света.

---

3. Петте инженерни инварианта

Петте режима се събират около малък, точен набор от инженерни изисквания. Те не са декларативни — те са проверими предикати, спрямо които може да се оцени всяка архитектура на съгласието.

3.1 Идентификатори, обвързани с личността

Субектът на данните трябва да контролира идентификатора, под който се записват неговите разрешения, пълномощия и статус на съгласие. Това е *предпоставката* за всеки друг инвариант: ако операторът притежава идентификатора, операторът притежава opt-out. EHDS Article 71(8) изрично изключва

регистри за повторна идентификация от страна на оператора; изискването за „пълен потребителски контрол” по eIDAS 2.0 Article 5a(14) назовава същото свойство на ниво портфейл. Без идентификатор, обвързан с субекта, разпространението, обратимостта и липсата на свързаност се свеждат до операторска политика.

3.2 Проверим opt-out с времеви печат

За всяко разрешение за данни системата трябва да знае точния момент на издаване и точния момент на оттегляне — и трета страна (регулатор, съд, последващ администратор) трябва да може да провери и двете, без да се доверява на журналите на оператора. EHDS Article 71(2) поставя остра времева граница: разрешенията, издадени преди opt-out, остават валидни; издадените след него са незаконни. Това не може да се приложи без защитена от промени, проверима от трети страни времева линия на статуса на съгласие на субекта.

3.3 Обратимост без повторна идентификация

Recital 54 от Регламента EHDS потвърждава, че opt-out е обратим (гражданите могат да се върнат към opt-in) и не е обвързан с форма (без минимален срок). Article 71(8) забранява на притежателя на данни да придобива допълнителни идентификационни данни единствено за изпълнение на opt-out. Двете разпоредби, прочетени заедно, създават строго ограничение: системата трябва да поддържа превключване на статуса на съгласие в двете посоки по преценка на гражданина, **без** притежателят на данни да изгражда паралелен регистър за повторна идентификация, за да следи кой е превключил кога. Всяка архитектура, изискваща „просто да се поддържа списък с гражданите, упражнили opt-out”, нарушава пряко разпоредбата на 71(8).

3.4 Разпространение между администратори

GDPR Article 17(2) задължава администратора, изпълняващ искане за заличаване, да предприеме „разумни стъпки, включително технически мерки”, за да уведоми последващите администратори, съхраняващи копия, реплики или препратки. EHDS Article 71, приложен върху вериги от разрешения с множество администратори, повишава изискванията: сигналът за opt-out трябва да достигне всеки Орган за достъп до здравни данни, всеки изследователски консорциум, всеки подизпълнител, получил данни по предходно разрешение. Разпространението не може да бъде само документална процедура — то трябва да бъде проверим артефакт, който последващите страни могат да проверят повторно.

3.5 Липса на свързаност

eIDAS 2.0 Article 5a(16)(b) изисква липса на свързаност между представянията на едни и същи идентификационни данни пред различни проверяващи. Оперативната последица: архитектура, при която дори една страна (включително упълномощен посредник) вижда всяка транзакция между проверяващите, не отговаря по дефиниция на изискването. Именно това свойство изключва федерираните доставчици на идентичност от гражданското ниво на системи, отговарящи на EHDS: доставчикът на идентичност по замисъл вижда всяко влизане и всяко представяне на

идентификационни данни. Федерацията може да покрие изискването за разпространение, но само като наруши изискването за липса на свързаност.

Тези пет инварианта образуват взаимосвързана система. **X.509 PKI не покрива нито един от тях на гражданско ниво. Федерираните IdP покриват разпространението, но само като нарушат липсата на свързаност. DKMS покрива всичките пет.** Това е твърдението за структурна стабилност, което останалата part на документа разглежда.

---

4. Капанът на Article 71(8)

Най-простият модел за изпълнение на opt-out — онзи, до който доставчик на здравна IT ще стигне в първия час от архитектурния разговор — е **централен регистър на идентификаторите на граждани, упражнили opt-out**. Всеки притежател на данни прави справка в регистъра преди обработването; ако идентификаторът на гражданина е в списъка, обработването спира. Лесно. Познато. Одитируемо.

Article 71(8) изцяло изключва този модел.

Разпоредбата забранява на притежателите на данни да придобиват допълнителни идентификационни данни единствено за изпълнение на opt-out. **„Списъкът с идентификаторите на граждани, упражнили opt-out" е по конструкция точно такъв регистър.** Той не съществува за друга цел освен повторното идентифициране на гражданите в отрицателния случай — за да се установи, че *конкретният гражданин е упражнил opt-out и следователно не може да бъде обработван*. Самият списък представлява нарушението, което е призван да предотврати.

Капанът е рекурсивен. Всеки опит за анонимизиране на регистъра (хеширане на идентификаторите, псевдонимизиране, съхранение в отделна доверена зона) отново въвежда първоначалния проблем: притежателят на данни все пак се нуждае от *някакъв* идентификатор, спрямо който да направи справка в списъка, и той трябва да бъде изводим от данните, с които притежателят вече разполага. Хешът не е анонимен за притежателя, разполагащ с входните данни; псевдонимът не е анонимен за притежателя, разполагащ с таблицата на свързаностите. Recital 54 засилва това, като изисква opt-out да бъде обратим и свободен по форма — т.е. регистърът трябва да поддържа превключване, което от своя страна изисква той да следи *кой* гражданин е превключил *кога* — именно записът за повторна идентификация, забранен от 71(8).

Последицата за доставчиците на здравна IT е категорична. **Всеки „модул за управление на съгласието", чиято архитектура почива на централен авторитетен списък на субекти, упражнили opt-out, е изключен от основното право на ЕС.** Това не е въпрос на UX дизайн; това е разликата между архитектура, способна да отговори на EHDS, и такава, която не може. Универсалните продукти за управление на съгласието, изградени на основата на модела с регистър — независимо дали са SaaS, on-premises или хибридни — ще се сблъскат с това ограничение при всяка транспозиция в държавите членки. Структурният отговор трябва да постави идентификатора под контрола на гражданина, така че притежателят на данни изобщо да не е принуден да поддържа регистър за повторна идентификация.

5. Тезата за DKMS

> **Децентрализираното управление на ключове е първата структурно стабилна основа за зачитане на opt-out от край до край — *в условия на междуорганизационен поток, след-разкриване и регулаторно наблюдение*.**

DKMS — изграден върху KERI, отворена спецификация на Trust over IP Foundation — поставя коренното доверие при гражданина, а не при централизиран орган. Гражданинът (или неговият wallet агент) притежава Autonomic IDentifier (AID), който е самоудостоверяващ се: той е изведен от публичен ключ под контрола на гражданина и неговата автентичност не зависи от никакъв регистратор. Всички пълномощия, предоставени на притежатели на данни, обработващи и последващи администратори, се свързват към този AID чрез Key Event Log (KEL) — структура само за добавяне, проверима от трети страни, съдържаща записи за ключовото състояние на гражданина, включително ротациите на ключове.

Оттеглянето в този модел не е искане, подадено до оператор. То е **ротация на ключ, извършена самостоятелно от гражданина**. Ротацията се публикува в KEL; от този момент всяка последваща страна, притежаваща идентификационни данни, обвързани с ключовото състояние преди ротацията, трябва да се пре-удостовери спрямо текущото ключово състояние на гражданина, за да продължи обработването. Съществуващите разрешения, издадени преди ротацията, продължават да действат там, където правното основание позволява (в съответствие с EHDS Article 71(2)); нови разрешения не могат да бъдат издавани под старото ключово състояние, тъй като то вече не е контролиращото ключово състояние на гражданина. Гражданинът е оттеглил бъдещото пълномощие архитектурно — не само процедурно — и всяка последваща страна, игнорираща публикуваната ротация, произвежда подписи, одитируеми като остарели.

Съпоставяне с петте инварианта:

Инвариант	Механизъм на DKMS
Идентификатори, обвързани с личността	AID е самоудостоверяващият се идентификатор на субекта; не е необходим индекс от страна на оператора
Проверим opt-out с времеви печат	KEL съдържа ключови събития, защитени от промени, с времеви печати
Обратимост без повторна идентификация	Opt-back-in = ротация на ключ, възстановяваща пълномощието; без паралелен регистър
Разпространение между администратори	KEL е публикуем; проверяващите трябва да правят повторна проверка в различни доверени зони
Липса на свързаност	

Инвариант	Механизъм на DKMS
	AID по контекст и идентификационни данни с избирателно разкриване избягват корелация между проверяващите

Сравнение със съществуващите алтернативи:

X.509 PKI обвързва идентичността със сертификат, издаден от удостоверяващ орган (CA). Гражданинът не е корен на доверието; CA е. Криптографската отмяна е движена от оператора (CRL/OCSP) и по подразбиране претърпява мек неуспех. Липсата на свързаност в различни контексти е структурно невъзможна — всяко представяне на сертификат е свързано чрез сериен номер, DN на издателя и DN на субекта. X.509 не покрива *нито един* от петте инварианта на гражданско ниво.

Федерирана IAM (OIDC, SAML). Доставчикът на идентичност е по замисъл инструментът за проследяване в различни контексти, забранен от eIDAS 2.0 Article 5a(16)(b). Федерацията може да покрие разпространението между администратори (единичното излизане изчиства сесиите надолу по веригата), но само като наруши изискването за липса на свързаност — всяко влизане минава през доставчика на идентичност, който вижда всяка разчитаща страна, която гражданинът посещава. Архитектурата може да покрие в най-добрия случай три инварианта и само за сметка на петия.

Централизиран KMS (AWS KMS, Azure Key Vault, GCP Cloud KMS). Подходящ за работни натоварвания в рамките на един tenant. Криптографското заличаване по NIST SP 800-88 §2.5 чрез Customer-Managed Keys е признато от регулаторите като окончателен метод за заличаване (EDPB Guidelines 01/2025; ENISA 2019 §4.2). Но след като данните напуснат границата на tenancy — в изследователски консорциум, последващ администратор, получател на данни за вторично използване — унищожаването на CMK от оператора не засяга копието. Разпространението между администратори остава нерешено. Schrems II / EDPB Recommendations 01/2020 Use Case 3 допълнително усложнява ситуацията: по дефиниция вносителят на данни не трябва да притежава ключовете.

DKMS не замества тези архитектури — той заема точната архитектурна ниша, която те не могат да запълнят. Централизиран KMS за заличаване в рамките на tenancy, X.509 за криптографска отмяна на ниво TLS, федерирана IAM за съгласие в обхвата на сесията — и DKMS за междуорганизационния, след-разкриващия слой, в който EHDS Article 71 реално действа.

---

6. Провалите на централизираните архитектури

Петте инварианта са проверими. Всяка основна централизирана архитектура на съгласието се проваля по структурно специфичен начин.

6.1 X.509 PKI не покрива нито един от петте инварианта на гражданско ниво

X.509 обвързва идентичността с удостоверяващ орган. CA генерира или съподписва сертификата на гражданина, притежава решението за издаване и контролира криптографската отмяна. Идентификаторите, обвързани с личността, се провалят в самия корен — подписът на CA е доверителният произход, а не подписът на гражданина. Opt-out с времеви печат е движен от оператора (гражданинът подава заявка за отмяна; CA решава дали да я приеме и кога да я публикува), а отмяната се разпространява само толкова бързо, колкото позволяват интервалите за опресняване на CRL или наличността на OCSP отговарящия — и двете по подразбиране претърпяват мек неуспех в браузърите. Обратимостта без повторна идентификация се проваля, тъй като повторното издаване изисква CA отново да валидира идентичността на субекта, което в здравен контекст означава, че CA трябва отново да придобие идентификационните данни, чието притежаване от страна на притежателя на данни EHDS Article 71(8) забранява. Разпространението между администратори зависи от правилната проверка на CRL/OCSP от всяка разчитаща страна — оперативна крехкост, доказана от инцидентите с DigiNotar и Comodo. Липсата на свързаност е структурно невъзможна: всеки X.509 сертификат носи сериен номер и DN на издателя, свързващи всяко представяне с едного и същи гражданин.

6.2 Федерираната IAM (OIDC/SAML) нарушава липсата на свързаност по дефиниция

OIDC и SAML осъществяват федерирана автентикация чрез доставчик на идентичност, посредничещ в отношенията между гражданина и разчитащата страна. Всяко влизане на гражданина при всеки проверяващ минава през доставчика на идентичност. Доставчикът на идентичност знае кой гражданин е достъпил коя услуга и кога. Това не е въпрос на конфигурация или нарушаване на политика — то е архитектурната функция на доставчика на идентичност. eIDAS 2.0 Article 5a(16)(b) изисква липса на свързаност между представянията на едни и същи идентификационни данни пред различни проверяващи; федерираният доставчик на идентичност е по конструкция единствената точка, в която всяко представяне се корелира. Федерацията може да осигури реално разпространение между администратори (Single Logout, OAuth Token Revocation, OIDC Back-Channel Logout) — но цената е нарушаването на инварианта за липса на свързаност при всяко представяне на идентификационни данни, за което посредничи доставчикът на идентичност.

6.3 Централизираният KMS не може да достигне разпространение между администратори

AWS KMS, Azure Key Vault и GCP Cloud KMS осигуряват одитируемо съхранение на ключове, FIPS 140-2 L3 / 140-3 backend-ове, планирано унищожаване на ключове (`ScheduleKeyDeletion`, soft-delete + purge, `DESTROY_SCHEDULED`) и envelope криптиране с разделяне на DEK/KEK. В рамките на един tenant това е напълно подходящ метод за заличаване по GDPR Article 17 — NIST SP 800-88 §2.5 изрично признава криптографското заличаване като метод за дезинфекция на ниво Purge, а EDPB Guidelines

01/2025 третират съхранението на ключове като определящо за това дали данните са анонимни за даден получател. Архитектурата работи **в рамките на границата на tenancy**.

Тя не преминава тази граница. След като данните са законосъобразно копирани в изследователски консорциум, последващ администратор или подизпълнител в друга доверена зона, унищожаването на KMS от страна на tenant-а не засяга копието. Разпространението по GDPR Article 17(2) се превръща в договорно задължение — документация, а не архитектура. Структурата на разрешителните вериги по EHDS Article 71 превръща тази празнота в структурна, а не случайна: всяко разрешение е потенциалното начало на верига с множество администратори, а централизираният CMK няма средства да стигне отвъд първото звено.

---

7. Границите на DKMS — задълбочена оценка

Тезата е структурна, а не абсолютна. Честното формулиране прави аргумента защитим; прекомерните твърдения го разрушават. Тезата за DKMS има четири ясни граници.

7.1 Производни данни — EDPB Opinion 28/2024

След като данните са трансформирани в производно — аналитични агрегати, тегла на ML модели, статистически извлечения, регулаторни доклади, вече подадени — унищожаването на ключа за изходния шифротекст не засяга производното. EDPB Opinion 28/2024 относно аспектите на защита на данните при AI моделите (прието на 17 декември 2024 г.) изрично потвърждава, че задълженията за заличаване не се разпространяват чисто върху теглата на модела след осъществяване на обучението. DKMS не е по-добър от централизирания CMK в това отношение. Ако разрешен изследователски консорциум е обучил модел върху данни, за които гражданинът по-късно е упражнил opt-out, теглата на модела остават. Архитектурният принос е одитируемостта на веригата на производство, а не ретроактивното им отмяна.

7.2 Вече направени архиви

Никаква архитектура за отмяна на активни ключове — DKMS или централизирана — не може да отзове данни, вече репликирани в неизменяеми архивни носители. Офлайн архиви, направени преди оттеглянето, стоят извън активното ключово пространство. Прагматичният отговор е документирано, планирано унищожаване на ключове при известен срок на съхранение — подход, одобрен от ICO, CNIL и BfDI като достатъчен за остатъчни лични данни в архиви. DKMS е съвместим с тази дисциплина; той не я замества.

7.3 Единичен недобросъвестен контрагент

В мрежа от N страни с една, която игнорира публикуваната ротация на ключа и продължава да действа въз основа на остарели идентификационни данни, DKMS осигурява **криминалистично разкриване** —

остарелите подписи са одитируеми след публикуваното събитие за ротация — но не и **предотвратяване**. Напълно несъдействащ последващ обработващ, който извлича открит текст и го съхранява извън ключовото обвиване, е извън архитектурния обхват на всяка система за управление на ключове. DKMS засилва доказателствената позиция на регулатора; той не премахва необходимостта от договорно, регулаторно или съдебно изпълнение срещу недобросъвестни страни. В сравнение с добре договорно управлявана централизирана CMK среда, DKMS засилва разкриването, но не елиминира нуждата от принудителни механизми срещу недобросъвестни участници.

7.4 Работни натоварвания в рамките на един tenant

За работни натоварвания, съществуващи изцяло в рамките на една доверена зона — вътрешни корпоративни данни при един администратор, single-tenant SaaS с tenant-обхватен CMK, публичен уеб TLS при CA/Browser Forum SLO за криптографска отмяна в рамките на 24 часа — криптографското заличаване по NIST SP 800-88 §2.5 чрез централизиран CMK е напълно подходящо. EDPB Guidelines 01/2025 и ENISA 2019 §4.2 признават унищожаването на ключа като окончателен метод за заличаване в рамките на tenancy. **Добавянето на DKMS към тези работни натоварвания налага операционна тежест без архитектурна полза.** Честният отговор е, че за single-tenant сценарии централизираната архитектура работи добре.

7.5 Решаващата граница

DKMS е доминиращото решение, когато **всичките четири** от следните условия са налице:

1. Данните преминават **поне две доверени зони**.
2. Съгласието трябва да **оцелее след-разкриването** (т.е. обработването продължава след границата).
3. Регулаторът третира **съхранението на ключове като определящо за изхода** (Schrems II / EDPB Recommendations 01/2020 Use Case 3 / EHDS Article 71(8)).
4. Страните прилагат DKMS **end-to-end** (проверяващ, игнориращ KEL, анулира веригата).

Извън тези четири условия централизираният CMK е рационалният избор, и признаването на това прави тезата за DKMS по-силна — не по-слаба — защото точно локализира твърдението там, където доказателствата го подкрепят. Тезата не е, че DKMS решава cookie банерите или заличаването в single-tenant SaaS. Тезата е, че DKMS е правилният структурен избор за *точно* онези случаи, от значение за презкантоналното, междуорганизационното, регулаторно наблюдаваното, след-разкриващото съгласие в здравеопазването.

---

8. Доказателство от production

Vereign поддържа DKMS архитектурата в production днес, с ясни уговорки за това какво е реализирано спрямо архитектурно проектираното.

SEAL е production комуникационният слой: криптирана доставка тип swarm за изходяща комуникация, с ключове за всяко отделно съобщение и агентност на получателя за дешифриране. SEAL обработва **800 000+ верифицирани съобщения всеки месец** за институционални потребители — каноничната production точка на опора за архитектурата. Всяко съобщение упражнява същия субстрат от ключови събития, залегнал в тезата за съгласието: ключване, контролирано от субекта, проверими от трети страни времеви печати и липса на свързаност по контекст между получателите.

Stargate — слоят за пълномощия, обвързан с AID, в който разрешенията за данни се свързват с KEL на гражданина — влиза в ранен production от юни 2026 г. с HIN като първо операционно внедряване. Stargate е повърхността на съгласието, описана в тезата: пълномощията, предоставени на притежатели на данни, са обвързани с AID на гражданина; ротацията на ключа от страна на гражданина се разпространява чрез KEL; последващите проверяващи правят повторна проверка. Внедряването при HIN е ограничено стартиране; **разказът за масовото разгръщане е запазен за след лятото на 2026 г.**, след като ранният production кохорт е натрупал операционни данни при реални регулаторни условия.

HIN мостовете позволяват оттеглянето да работи съвместно с контрагенти, използващи X.509, чрез KERI-обвързания S/MIME мост, документиран в базата знания за сигурност на имейла. Това е прагматичното признание, че DKMS ще работи заедно с — а не ще замени за нощ — съществуващата X.509 здравна инфраструктура.

FHIR-over-Stargate е архитектурно разработен — production внедряването зависи от onboarding от страна на болниците; най-ранната реалистична дата е септември 2026 г. Архитектурното решение е наистина здраво: FHIR ресурсите, преминаващи през Stargate, наследяват модела за пълномощия, обвързан с AID, така че статусът на съгласие на ниво ресурс е там, където гражданинът го контролира. Но инженерингговото усвояване от страна на болниците — интеграция с клинични системи, регулаторно одобрение, операционно управление — е начинание за няколко тримесечия. Не твърдим, че FHIR-over-Stargate е реализиран. Твърдим, че е следващата планирана стъпка с известна най-ранна дата, и очакваме операционното внедряване да изостава от архитектурната готовност с измерим интервал. Смесването на двете е провалният модел, за чието предотвратяване е написан настоящият документ.

Production-ната история е важна, защото именно тя разграничава тезата от презентация. Инженерните организации редовно се сблъскват с аргумента централизация срещу децентрализация; рядко обаче срещат децентрализация, работеща в реална институционална среда, под реален регулаторен надзор, в регулирана индустрия. Субстратът за верифицирани съобщения обработва реален институционален трафик достатъчно дълго, за да разкрие операционните ъгли на DKMS — дисциплина при ротация на ключове, discovery между организации, съхранение на одитни журнали, агентност на получателите — и тези ъгли са изшлифовани в production, а не в теория. Когато Stargate влезе в ранен production от юни 2026 г., ще работи на същия субстрат. Архитектурният аргумент следователно не е прогноза; той е екстраполация от наблюдавани операции в практическата експлоатация.

9. Пет инцидента, доказващи структурния модел

Пет инцидента — три от 2026 г., два основополагащи по-стари случая — илюстрират защо централизираните архитектури се провалят под регулаторен натиск и как провалът е структурен, а не операционен.

9.1 Kaiser Foundation Health Plan — спогодба за 47,5 млн. USD (2026)

Kaiser Foundation Health Plan постигна спогодба за 47,5 милиона USD по колективен иск, свързан с проследяване чрез пиксели в пациентски портали, с окончателно одобрение, влязло в сила на 30 април 2026 г. Ищците твърдяха, че пиксели за проследяване на Meta и Google, вградени в автентикирания пациентски портал на Kaiser, са предавали защитена здравна информация на рекламни платформи на трети страни — включително диагнози, видове посещения и запитвания за медикаменти — заедно с идентификатори, достатъчни за повторно свързване на данните с конкретни пациенти. Архитектурният провал е точен: съгласие на пациента съществуваше на регистрационния слой на портала, но потокът от данни беше определен от вградените SDK-та, а не от заявеното предпочитание на пациента. Оттеглянето на съгласие не засегна пикселните събития, вече предадени, и пациентът нямаше архитектурно средство да открие или отмени потоците към трети страни.

9.2 Sutter Health — спогодба за 21,5 млн. USD (2026)

Sutter Health постигна спогодба за 21,5 милиона USD по същия модел на производство, с окончателно одобрение на 27 февруари 2026 г. Паралелни спогодби са сключени или предстоят срещу BJC HealthCare, Northwell Health, Catholic Health, Aspirus и SSM Health при по същество идентични факти. Списъкът на спогодбите за 2025–2026 г. като цяло е водещият индикатор: всяка голяма американска здравна система, вградила пиксели за проследяване на трети страни в повърхности, насочени към пациентите, сега плаща за архитектурното отсъствие на криптографски граници на ниво пациент при потока от данни. Съгласието беше квадратче за отметка; потокът беше решен другаде.

9.3 Национален opt-out на NHS данни (NDOO) — Неретроактивност, 2018–2021

NHS England консолидира наследените opt-out от Тип 1 и Тип 2 в Национален opt-out на данни (NDOO) от 2018 г. с нормативна сила. Програмната документация и коментарите на ICO впоследствие потвърдиха, че opt-out е демонстративно **неретроактивен**: данните, вече извлечени от GP системите преди регистрирането на opt-out от гражданина, са останали в изследователски набори от данни и са можели да продължат да бъдат обработвани. NHS Digital не разполагаше с техническа инфраструктура за отзоваване на вече извлечени записи. Програмата-наследник GPDPR (General Practice Data for Planning and Research) беше планирана да стартира на 1 юли 2021 г. и беше отложена за неопределено в юни 2021 г., именно защото нямаше технически начин за заличаване на вече извлечени GP данни при последваща регистрация на opt-out по Тип 1. Към 2026 г. извличането все още не е започнало.

Архитектурният урок: когато операторът притежава пътя на данните, „ветото на пациента” няма механизъм за изпълнение — и политическият механизъм се срива под собствената си криминалистична тежест.

9.4 SingHealth — 1,5 млн. компрометирани записа (2018)

Публичният доклад на Комисията по разследване на Сингапур относно кибератаката срещу Singapore Health Services (10 януари 2019 г.) установи, че 1,5 милиона пациентски записа на SingHealth са компрометирани, включително личното здравно досие на министър-председателя на Сингапур. Техническото заключение е архитектурното: не е имало **разделение** в системата за електронни медицински записи на SingHealth. След като атакуващият е достигнал приложението Allscripts Sunrise чрез привилегирован служебен акаунт, всички пациентски записи са станали достъпни. Съгласието на пациента беше политически артефакт на слоя за достъп; слоят данни **нямаше криптографска граница на ниво пациент**. Повърхността на нарушението беше именно отсъствието на тази граница.

9.5 Компрометиране на удостоверяващ орган DigiNotar (2011)

Разследването на Fox-IT, публикувано като доклада „Black Tulip” (13 август 2012 г.), установи, че всичките осем CA сървъра на DigiNotar са компрометирани. Издадени са 531+ фалшиви сертификата, включително wildcard сертификат `*.google.com`, използван за атака „мъж по средата” срещу приблизително 300 000 ирански потребители на Gmail. Мярката по отстраняване — недоверие към DigiNotar — беше предприета едностранно от Mozilla, Microsoft и Google и разпространена до крайните потребители чрез актуализации на хранилището на корени. Собствената верига на нидерландското правителство Staat der Nederlanden – G2 беше пренебрегната при първоначалното премахване и изисква допълнителна намеса. Крайните потребители **нямаха никаква агентност** при вземане на решенията за доверие на нито един етап: нито при издаването, нито при разкриването, нито при отстраняването. Те научиха за компрометирането, когато собствените им услуги спряха да работят.

При всеки централизиран инцидент е налице един общ белег: потребителят не е имал архитектурна свобода на действие. Пациентите на Kaiser и Sutter не контролираха пикселния поток. Пациентите на NHS не можеха да отзоват извлечените данни. Пациентите на SingHealth нямаха криптографска граница на ниво запис. Крайните потребители на DigiNotar не можеха да гласуват за решенията за доверие. Моделът е структурен и се потвърждава в продължение на пет десетилетия свидетелства от инциденти, независимо от регулатора, сектора или юрисдикцията.

---

10. Заключение и как да се свържете с нас

Opt-out е преминал от политическа декларация до приложимо законово право съгласно EHDS Article 71, GDPR 7(3) и 17(2), eIDAS 2.0 5a(14)/(16)(b), швейцарски FADP и HFG и германски PDSG. Пет инженерни инварианта следват пряко от тях: идентификатори, обвързани с личността, проверим opt-out

с времеви печат, обратимост без повторна идентификация, разпространение между администратори и липса на свързаност. X.509 PKI не покрива нито един от тях на гражданско ниво; федерираната IAM покрива разпространението само като нарушава липсата на свързаност; централизираният KMS покрива single-tenant случая, но не може да достигне отвъд доверените зони. **DKMS е първата структурно стабилна основа за зачитане на opt-out от край до край в условия на междуорганизационен поток, след-разкриване и регулаторно наблюдение** — с ясни граници около производни данни, архиви и единичен недобросъвестен контрагент. Списъкът на спогодбите за 2025–2026 г. (Kaiser, Sutter, BJC, Northwell, Catholic Health, Aspirus, SSM Health) е живото доказателство, че при всяка централизирана архитектура под подобен регулаторен натиск е налице един общ белег: потребителят не е имал архитектурна свобода на действие.

Ако отговаряте за архитектурата на съгласието в здравна IT среда, изправена пред транспозиция на EHDS, изпълнение на швейцарски EGDG / BDG или операции по германски PDSG, Vereign предлага 30-минутен преглед на архитектурата на съгласието. Ще картографираме текущата ви повърхност на съгласие спрямо петте инварианта, ще идентифицираме капаните на Article 71(8) в пътната ви карта и ще определим точния обхват, в който DKMS е — и не е — правилният архитектурен отговор. **Свържете се с нас: contact@vereign.com.**

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