

BIM MAGAZIN

DIGITAL UND NACHHALTIG PLANEN-BAUEN-BETREIBEN

Artikel:

Der Datenraum im Bauwesen

Eine Kooperation von:



Der Datenraum im Bauwesen – eine vertrauenswürdige Infrastruktur für die Zukunft der digitalen Zusammenarbeit



Dr. Jan Tulke, Geschäftsführer planen-bauen 4.0
© Joana Rottleuthner



Franziska Karsten M.A., Kommunikation und Politik
© Simone M. Neumann



Dr. Martin Heß, Senior-Projektleiter Innovation und Softwareentwicklung
© Fotostudio Hirsch



Die Bauwirtschaft steht vor der Chance, digitale Informationen zukünftig projekt- und unternehmensübergreifend verfügbar zu machen und daraus wirtschaftlich nutzbare Mehrwerte zu erzielen. Planungsmodelle, Produktdaten, Nachweise, Zertifikate oder Umweltkennwerte sind zentrale Entscheidungsgrundlagen. Ihr wirtschaftlicher Mehrwert entsteht jedoch erst dann, wenn sie kontrolliert und zweckgebunden ausgetauscht werden können.

1. Von projektbezogenem Datenaustausch zur digitalen Wertschöpfung

Ein Datenraum für das Bauwesen stellt hierfür die technische und organisatorische Infrastruktur bereit. Er ermöglicht einen standardisierten, souveränen und kryptografisch abgesicherten Datenaustausch zwischen Planung, Ausführung und Betrieb.

Im Grundprinzip ähnelt der Datenraum dem Internet: Im Mittelpunkt steht das gezielte Auffinden und der Austausch von Informationen zwischen zwei Parteien sowie die Möglichkeit, Bedingungen für die Datennutzung verbindlich zu definieren. Voraussetzung ist dabei, dass Identitäten und Zugriffsberechtigungen technisch überprüfbar sind.

2. Was unter einem Datenraum zu verstehen ist

Ein Datenraum ist keine zentrale Plattform, keine einzelne Softwarelösung und kein Cloud-Speicher. Er beschreibt die Gesamtheit von Akteuren, die sich auf gemeinsame technische, organisatorische und rechtliche Regeln für den Datenaustausch verständigt haben.

Charakteristische Merkmale sind:

- » dezentrale Datenhaltung in den Systemen der jeweiligen Organisationen,
- » standardisierte Beschreibungen von Teilnehmern und Datenangeboten,
- » eine verlässliche, kryptografisch abgesicherte Identifikation aller Akteure,
- » sowie individuelle Zugriffsregeln und Nutzungsbedingungen, die festlegen, auf welche Daten zugegriffen werden darf und wie diese verwendet werden dürfen.

Der Datenaustausch erfolgt dezentral zwischen Datenbesitzer und Datennutzer; zentrale Dienste unterstützen lediglich Auffindbarkeit und Identitätsprüfung.

Der Datenraum selbst speichert oder verarbeitet keine operativen Nutzdaten zentral; diese verbleiben bei den jeweiligen Dateneinhabern.

Um die Grundfunktionalitäten von Datenräumen branchenübergreifend und interoperabel zu etablieren, sind gemeinsame Konzepte erforderlich. Diese werden insbesondere von Initiativen wie [Gaia-X auf europäischer Ebene und der International Data Spaces Association \(IDSA\)](#) auf internationaler Ebene entwickelt.

3. Warum ein Datenraum für das Bauwesen erforderlich ist

Bauprojekte sind von hoher Komplexität, zahlreichen Beteiligten und projektbezogenen Netzwerken geprägt. Gleichzeitig steigen die Anforderungen an Transparenz, Nachhaltigkeit und Nachweisführung. ESG-Kennzahlen sowie Umwelt- und Produktdaten müssen belastbar, aktuell und prüfbar bereitgestellt werden.

Entlang der Liefer- und Wertschöpfungskette wächst zudem der Bedarf an aktuellen Informationen, um Materialflüsse zu steuern, Risiken frühzeitig zu erkennen, Stillstandskosten zu reduzieren und benötigte Informationen gezielt abrufen zu können.

Informationen entstehen in jeder Phase eines Projekts und lassen sich, einmal erzeugt, häufig mehrfach nutzen. Fehlen standardisierte Austauschmechanismen, entstehen Medienbrüche und redundante Erfassungen.

Ein strukturierter Austausch über einen gemeinsamen Datenraum schafft hier Abhilfe. Er ermöglicht die kontrollierte Weiterverwendung von Informationen, eröffnet Potenziale zur Monetarisierung von Datenangeboten und fördert neue Formen der Zusammenarbeit entlang der gesamten Liefer- und Wertschöpfungskette.

4. Prinzipien und Konzepte des Datenaustauschs

Unabhängig vom Anwendungsbereich basieren Datenräume auf drei technischen Grundprinzipien: Dezentralität, Datensouveränität und kryptografisch gesicherte Identität.

4.1. Dezentralität

Daten verbleiben physisch in den Systemen der jeweiligen Organisationen. Eine zentrale Datensammlung ist nicht vorgesehen. Der Datentransfer erfolgt verschlüsselt direkt zwischen den beteiligten Parteien auf Basis standardisierter Protokolle.

Die technische Umsetzung erfolgt über sogenannte Konnektoren. Sie fungieren als gesicherte Schnittstelle zwischen interner IT-Infrastruktur und Datenraum. Bestehende Systeme wie BIM-Authoring-Tools, ERP-Lösungen oder Fachanwendungen werden über den Konnektor angebunden – vorausgesetzt, sie integrieren den Konnektor beziehungsweise unterstützen die entsprechenden Schnittstellen.

Der Datenaustausch erfolgt dann aus diesen Anwendungen heraus; eine separate Plattformoberfläche ist nicht erforderlich. Der Datentransfer wird als verschlüsselte Punkt-zu-Punkt-Verbindung zwischen den beteiligten Konnektoren aufgebaut. Grundlage ist ein standardisiertes Übertragungsprotokoll, das [Dataspaces Protocol](#) der IDSA.

Der Connector übernimmt mehrere Aufgaben:

- » Authentifizierung und Identifikation der beteiligten Kommunikationspartner bzw. Systeme,
- » Aufbau einer verschlüsselten Direktverbindung zwischen den Parteien,
- » maschinelle Verarbeitung und Prüfung von Datennutzungsbedingungen (Policy Enforcement),
- » Durchführung des Transfers auf Basis standardisierter Protokolle (IDSA),
- » sowie das Logging des Datenaustauschs.

Vor der Übertragung werden die vereinbarten Nutzungsbedingungen technisch validiert. Dazu gehören insbesondere Zweckbindung, Nutzungsdauer und gegebenenfalls definierte Weitergabebeschränkungen. Erst wenn diese Prüfung erfolgreich ist, wird die Datenfreigabe ausgelöst.

Das Logging erfasst Transaktionsmetadaten wie beteiligte Identitäten, Zeitstempel und referenzierte Nutzungsbedingungen. Die Protokolle verbleiben jeweils bei den beteiligten Organisationen.

4.2. Datensouveränität

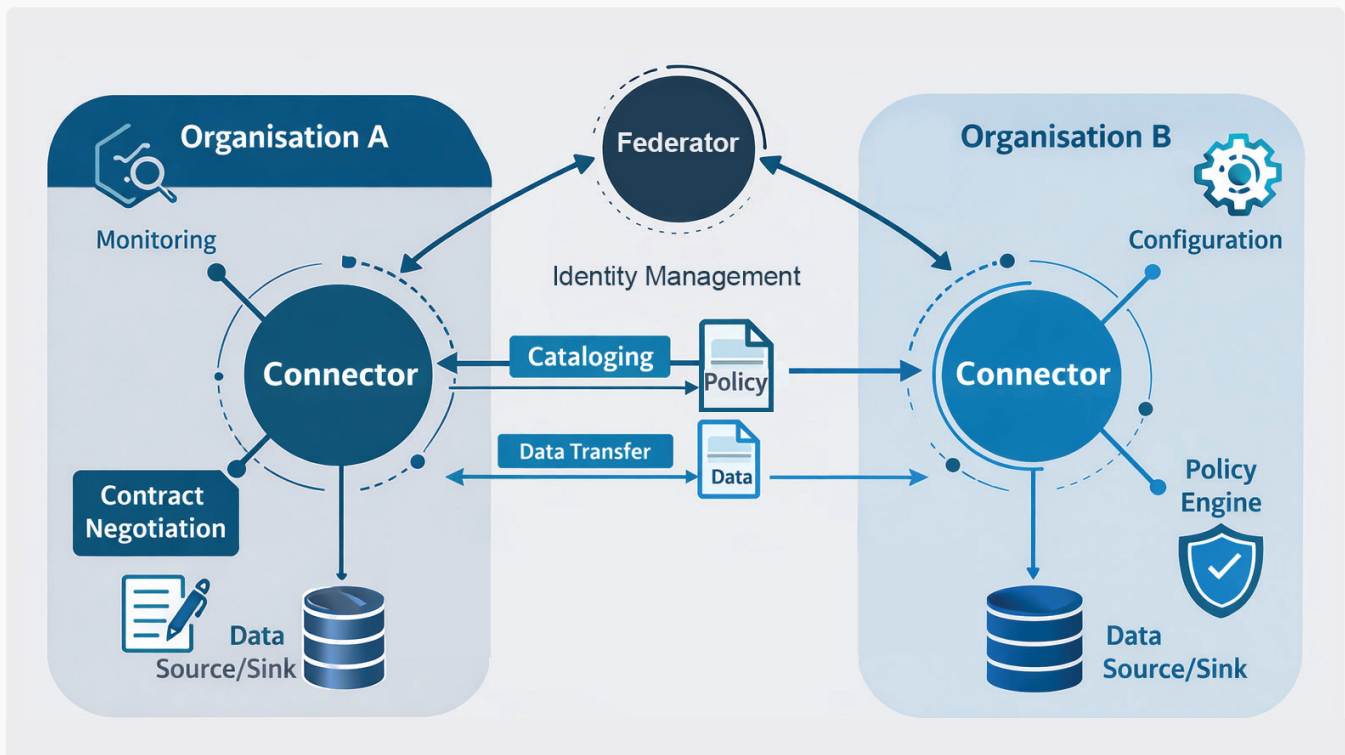
Die dezentrale Architektur bildet die Grundlage für Datensouveränität. Der Datenbesitzer kann zudem in seinen Datennutzungsbedingungen (Policies) definieren,

- » welche (Teil-)Daten geteilt werden,
- » zu welchem Zweck,
- » unter welchen Bedingungen z. B. Nutzungsdauer, Weitergabe,
- » und ob eine Vergütung erfolgt.

Diese Bedingungen werden vor dem Datentransfer maschinell geprüft und sind integraler Bestandteil der Transaktion.

”

Unabhängig vom Anwendungsbereich basieren Datenräume auf drei Grundprinzipien: Dezentralität, Datensouveränität und kryptografisch gesicherte Identität.“



© basiert auf: www.internationaldataspaces.org/idsa-data-space-connector-report/

Da der Austausch direkt zwischen den Parteien erfolgt, kann keine zentrale Instanz auf Inhalte zugreifen oder Datenaustauschbeziehungen auswerten. Die Kontrolle verbleibt vollständig beim Dateninhaber.

4.3. Digitale Identitäten und Verifiable Credentials

Ein zentraler Aspekt von Datenräumen ist die Schaffung von Vertrauen zwischen den datenaustauschenden Akteuren. Voraussetzung ist die verlässliche Feststellung, wer mit wem interagiert und mit welchen Berechtigungen. Technisch geschieht dies über digitale Signaturen und organisationsübergreifend nutzbare Identitätsmechanismen, vergleichbar mit Zertifikaten im Internet.

Eine zentrale Rolle spielen dabei sogenannte [Verifiable Credentials \(VC\)](#). Ein Verifiable Credential ist ein von der World Wide Web Consortium (W3C) standardisiertes Datenformat für digitale Nachweise.

Ein VC enthält neben den eigentlichen inhaltlichen Aussagen (z. B. Eigenschaften, Rollen oder Berechtigungen) auch Metadaten zum Aussteller/Inhaber, Gültigkeitszeiträume sowie kryptografische Schlüssel. Das gesamte Objekt wird vom Aussteller digital signiert und ist dadurch technisch überprüfbar.

Vor dem Datenaustausch weisen sich die beteiligten Parteien gegenseitig aus, indem sie entsprechende Verifiable Credentials oder vergleichbare signierte Identitätsnachweise austauschen. Diese werden von vertrauenswürdigen Stellen – etwa Identity-Providern, Kammern, Behörden oder Zertifizierungsstellen – ausgestellt und kryptografisch signiert. Die empfangende Partei prüft automatisiert die Signatur, die Integrität des Nachweises sowie die Vertrauenskette des Ausstellers. Auf dieser Grundlage wird bewertet, ob die bestätigten Merkmale den Zugriffsregeln (Policies) des Datenraums und regulatorischen Anforderungen entsprechen. Erst nach erfolgreicher Prüfung werden angefragte Daten, etwa Inhalte eines digitalen Produktpasses, freigegeben.

Jede Organisation im Datenraum verfügt über ein kryptografisches Schlüsselpaar: Der private Schlüssel dient zur Signatur, der öffentliche Schlüssel zur Prüfung von Echtheit und Integrität. Wird ein Verifiable Credential oder ein Datenangebot signiert, kann technisch nachgewiesen werden, dass es vom angegebenen Aussteller stammt und nach der Signatur nicht verändert wurde.

Zur eindeutigen Zuordnung öffentlicher Schlüssel zu einer digitalen Identität werden häufig [Decentralized Identifiers \(DID\)](#) verwendet.

Eine DID verweist auf ein DID-Dokument, in dem die aktuell gültigen öffentlichen Schlüssel sowie weitere Identitätsinformationen hinterlegt sind (z. B. did:web:planen-bauen40.de). Über dieses Dokument kann der zur Signatur gehörende öffentliche Schlüssel automatisiert aufgelöst und für die Prüfung herangezogen werden.

Die Identitätsbestätigung kann unmittelbar kryptografisch verifiziert werden. Dies erfolgt durch die automatisierte Prüfung einer digitalen Signatur und der zugehörigen Zertifikats- und Vertrauenskette durch sog. Trusted Authorities. Dazu zählen Datenraumbetreiber sowie Zertifikatsanbieter wie [DigiCert](#) oder [D-Trust](#), die für die Identitätsprüfung unter anderem Extended-Validation-Zertifikate (EV-SSL) einsetzen.

Gerade im Bauwesen sind neben der reinen Organisationsidentität konkrete Berechtigungen entscheidend, etwa Bauvorlageberechtigungen, Präqualifizierungen oder Kammermitgliedschaften. Auch diese können als Verifiable Credentials abgebildet werden. Eine berechtigte Stelle (z. B. Kammer, Verband oder Behörde) stellt einen digitalen Nachweis im standardisierten VC-Format aus und signiert ihn mit ihrem privaten Schlüssel. Die inhaltliche Aussagekraft, d.h. welche Eigenschaften oder Prüfungen bestätigt werden, ergibt sich aus dem jeweiligen Zertifizierungsverfahren und der Reputation der ausstellenden Stelle, während die technische Echtheit und Unveränderbarkeit kryptografisch überprüfbar sind.

Auf diese Weise entstehen im Datenraum technisch prüfbare Identitäten und Berechtigungsnachweise, deren inhaltliche Aussagekraft vom jeweiligen Zertifizierungsverfahren und der ausstellenden Stelle abhängt.

4.4. Föderierte Dienste und Governance

Der Datentransfer selbst erfolgt dezentral zwischen den beteiligten Organisationen. Damit ein solches verteiltes System dauerhaft interoperabel, auffindbar und regelkonform funktioniert, sind jedoch gemeinsame Rahmenkomponenten erforderlich. Diese Komponenten speichern keine operativen Projektdaten, sondern strukturieren und koordinieren das Zusammenspiel der Teilnehmer.

Registries verwalten technische Identitätsinformationen und Endpunkte von Teilnehmern. Sie unterstützen die eindeutige Zuordnung von Organisationen, Konnektoren oder Diensten innerhalb des Datenraums.

Im Vergleich zur Sicherstellung der Identität (vgl. Kapitel 4.3) stellen Registries die organisatorische und technische Auffindbarkeit dieser Identitäten sicher.

Ein zentrales Element ist der Katalog der Datenangebote (Catalog). In ihm werden Datenprodukte, Services oder Zertifizierungen mit beschreibenden Informationen (Metadaten) registriert. Dazu gehören etwa Angaben zum Anbieter, zur Art der Daten, zu Schnittstellen oder zu grundlegenden Nutzungsbedingungen. Der Katalog dient der Auffindbarkeit verfügbarer Angebote, ohne dass die eigentlichen Daten zentral vorgehalten werden. Er ermöglicht es Organisationen, gezielt nach relevanten Datenquellen oder Diensten zu suchen und eine Anfrage einzuleiten.

Ein weiterer Baustein sind standardisierte Policy-Vorlagen. Sie dienen dazu, Datennutzungsbedingungen strukturiert und interoperabel zu formulieren. Anstatt individuelle Vertragslogiken jedes Mal neu zu definieren, können vordefinierte Muster verwendet werden, die maschinell auswertbar sind und eine konsistente Anwendung innerhalb des Datenraums ermöglichen.

Auf dieser Grundlage können auch datenraumbezogene Anwendungen (Apps) entstehen. Solche Anwendungen greifen über Konnektoren auf Datenangebote zu und setzen auf den beschriebenen Identitäts- und Policy-Mechanismen auf. Sie nutzen die Infrastruktur des Datenraums, ohne selbst eine zentrale Datenhaltung zu übernehmen. Beispiele sind Anwendungen zur CO₂-Bilanzierung, zur qualifikationsbasierten Freigabeprüfung oder zur Integration externer Produktdaten in Fachsysteme.

Zur formalen Sicherstellung von Regeln können Notary- oder Compliance-Dienste eingesetzt werden. Diese prüfen die Einhaltung definierter technischer und organisatorischer Anforderungen. Dazu gehören etwa die Validierung von Verifiable Credentials oder die Überprüfung der Konformität mit Referenzarchitekturen wie der [Gaia-X-Architektur](#). Gaia-X definiert Richtlinien für die Architektur und den Betrieb eines Datenraums nach [europäischen Werten](#). Ziel ist es, gemeinsame Konzepte und Open-Source-basierte Softwarelösungen für die Umsetzung und den Betrieb von Datenräumen bereitzustellen.

Die übergreifende Koordination der Komponenten eines Datenraums erfolgt auf zwei Ebenen: organisatorisch und technisch. Die organisatorische Verantwortung liegt in der Regel beim Datenraumbetreiber – etwa einer Branchenvereinigung oder einer steuernden Instanz. Er definiert die Governance-Regeln, Teilnahmebedingungen, Compliance-Vorgaben sowie technische Mindestanforderungen für Interoperabilität und Sicherheit. Dabei betreibt er selbst keine operative Datenaustauschplattform und erhält keinen Zugriff auf projektspezifische oder geschäftskritische Daten.

”

Ein zentraler Aspekt von Datenräumen ist die Schaffung von Vertrauen zwischen den datenaustauschenden Akteuren.“

Seine Aufgabe besteht darin, einen verbindlichen Ordnungsrahmen für ein dezentrales und souveränes Datenaustauschsystem zu schaffen.

Davon zu unterscheiden ist die Rolle des Förderators. Dieser übernimmt technische Basisdienste des Datenraums, wie Verzeichnis- und Suchdienste, über die Teilnehmer, Datenangebote oder Services auffindbar sind. Der Förderator ermöglicht somit die technische Vermittlung und Auffindbarkeit innerhalb des Ökosystems, ohne selbst in den operativen Datenaustausch oder die inhaltliche Datenhaltung eingebunden zu sein.

Durch die klare Trennung zwischen Governance-Verantwortung und technischen Basisdiensten bleibt der operative Datenaustausch dezentral organisiert, da Daten ausschließlich zwischen den Teilnehmern ausgetauscht werden. Gleichzeitig sorgen verbindliche Regeln sowie gemeinsam genutzte Basisdienste für Interoperabilität, Auffindbarkeit und einen verlässlichen technischen Rahmen.

5. Datenaustausch im Projekt und in der Lieferkette

Projektbezogen lassen sich Planungsstände, Nachweise oder Prüfvermerke bereitstellen, deren Nutzung klar auf den Projektkontext begrenzt ist. Darüber hinaus können Daten projektübergreifend genutzt werden, etwa Umweltkennwerte von Bauprodukten oder Qualifikationsnachweise von Unternehmen. Ein typischer Anwendungsfall ist die CO₂-Bilanzierung entlang der Lieferkette, bei der dezentrale Daten zu einem Gesamtbild zusammengeführt werden, ohne sensible Informationen zentral zu speichern.

Konkrete Use Cases reichen von digitalen Bauakten über automatisierte Freigabeprozesse bis hin zu durchgängigen Nachweisketten. Entlang der Liefer- und Wertschöpfungskette erleichtert ein Datenraum die Zusammenarbeit zwischen Planern, ausführenden Unternehmen, Subunternehmern und Behörden erheblich.

6. Fazit und Ausblick

Der Datenraum ist keine weitere IT-Anwendung, sondern eine Rahmeninfrastruktur für souveränen und automatisierbaren Datenaustausch, an die sich jede Organisation der Bau- und Immobilienbranche per Konnektor anschließen kann.

Er schafft die Grundlage für durchgängige digitale Prozesse über Projekte, Organisationen und Wertschöpfungsketten hinweg. Informationen, die bislang isoliert in einzelnen Systemen entstehen, können strukturiert, zweckgebunden und kryptografisch abgesichert ausgetauscht werden.

Durch die systemübergreifende Bereitstellung einheitlicher Daten und die nahtlose digitale Vernetzung aller Projektbeteiligten können bestehende Prozessbrüche reduziert werden, Nachweise können automatisiert geprüft und Qualifikationen maschinell abgeglichen werden.

Ein weiterer Entwicklungsschritt liegt in der Integration digitaler und physischer Prozesse. Physische Daten, die durch Sensoren auf Baustellen oder in der Vorfertigung erfasst werden, könnten über Konnektoren in den Datenraum eingebunden werden. So könnten digitale Zwillinge von Bauwerken oder Bauteilen kontinuierlich mit aktuellen Daten aus Planung, Ausführung oder Betrieb verknüpft werden. Dadurch lassen sich Baufortschritt, Qualitätsanforderungen oder Betriebszustände kontinuierlich bewerten.

Strukturierte und verlässlich signierte Daten schaffen zudem die Voraussetzung für weitergehende Automatisierung, etwa bei Freigaben, Materialdisposition oder qualifikationsbasierten Zugriffsentscheidungen. Auch der Einsatz robotischer Systeme auf der Baustelle oder in der Vorfertigung profitiert von konsistenten, standardisiert zugänglichen Daten.

🔗 **Gaia-X** liefert dafür den europäischen Rahmen für Vertrauen und Interoperabilität. Der eigentliche Mehrwert entsteht jedoch erst im fachlich ausgestalteten Bau-Datenraum: Dort werden branchenspezifische BIM-Anwendungsfälle, verbindliche Datenmodelle und klare Governance-Regeln so definiert, dass Informationen strukturiert, nachvollziehbar und projektübergreifend austauschbar sind.

Datenräume, wie z.B. im Projekt Construct-X entwickelt, können somit beitragen, dass digitale Methoden und Automatisierung dauerhaft skalierbar und regelkonform im Planen, Bauen und Betreiben verankert werden.

| BIM MAGAZIN - März 2026

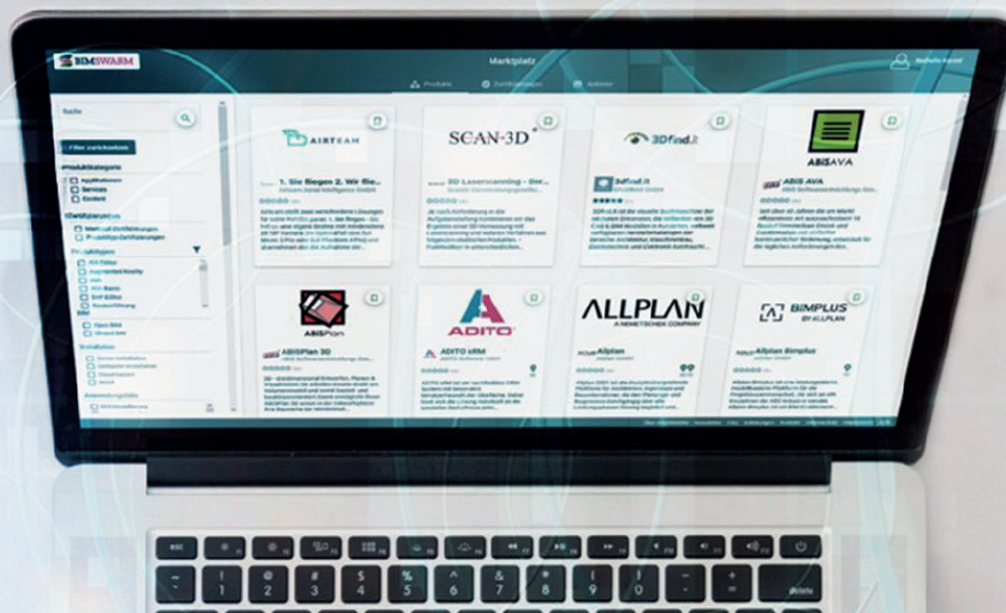
Datenräume werden derzeit im Rahmen öffentlich geförderter Projekte in vielen Branchen aufgebaut.

Construct-X ist ein vom Bundesministerium für Wirtschaft und Energie (BMWE) sowie der Europäischen Union gefördertes Projekt im Rahmen von IPCEI-CIS. Ziel ist die Entwicklung eines Datenraumes für die Bauwirtschaft.

Erarbeitet werden Referenzarchitekturen, OpenSource Komponenten, standardisierte Schnittstellen und konkrete Anwendungsfälle wie digitale Produkt- und Materialdatenpässe.

Weitere Informationen:

🔗 construct-x.org



Die Zukunft des Bauens ist digital.

BIMSWARM ist die Brücke zwischen Anbietern und Anwendern von Bau-IT.



Für Software-Anbieter:

- ◆ Präsentieren Sie Ihre Bau-IT-Produkte auf einem neutralen branchenspezifischen Marktplatz.
- ◆ Generieren Sie qualifizierte Leads für Ihre Produkte mit integrierten Kategorisierungskriterien.
- ◆ Steigern Sie die Sichtbarkeit Ihrer Angebote, um Kunden zu gewinnen.

Für Anwender aus Planung, Bau und Betrieb:

- ◆ Finden und vergleichen Sie passende Software-Lösungen – nach Anwendungsfall, Schnittstellen und Qualitätskriterien.
- ◆ Nutzen Sie die marktübergreifende Suche und wählen Sie die passende IT für Ihre BIM-Prozesse aus.
- ◆ Finden Sie transparente Informationen zu Funktionalitäten, Zertifikaten und Kompatibilitäten von Bau-IT-Produkten.