# Datum for Enterprise

Datum was founded in response to a shift in the way governments and their citizens are thinking about how companies handle customer data. As data has become both increasingly valuable to businesses and available to criminals, it's become apparent that new technology and tools are needed to protect individuals and enable them to control and benefit from this burgeoning digital asset. New opportunities are now possible to unlock the potential for rewarding consumers for sharing more about themselves, increasing the quality and verification of data, while saving billions lost to fraud, data breaches and litigation.

As a blockchain software and services company Datum provides custom solutions to enterprise businesses in the area of secure, privacy-forward, trust less data storage and management. This approach enhances customer privacy, customer consent, identity management and identity verification in turn reducing enterprise liability for fraud and large scale data breaches.

Datum is a Layer 2 blockchain technology. A decentralized data store that offers scalability and high availability with a ready-to-use SDK for interacting with an underlying blockchain. Datum enables tracking and access control of non-blockchain data through a secure blockchain layer. Currently based on Ethereum, Datum is coming to other leading blockchain platforms such as Hyperledger and Quorum.

Datum is a good choice for companies that want to control the liability of storing and handling PII while retaining user-permissioned access to data as needed.

## Datum Technology Stack

- Proof of Authority (POA) based distributed ledger technology (DLT)
- Distributed and end-to-end encrypted key-value data store
- Datum SDK
- Datum ID - iPhone and Android mobile app
- Datum Blockchain Indexer and Explorer

## Use Cases

- Customer Registration
- Data Anchoring
- Data Verification
- Identity Utilities
- Secure Messaging
- User Consent Management
- GDPR Compliance

## Industries

- Accounting
- Digital Advertising
- Education
- Financial Services
- Healthcare
- Insurance
- Life Sciences
- Manufacturing
- Telecom

Datum was developed as an open-source technology intended to act as public infrastructure. The technology is now being commercialized to suit the needs of enterprise customers. Datum is currently seeking to co-create proof-of-concepts with research and innovation teams at companies who value customer privacy, data security and fraud prevention – **please contact sales@datum.org for more information.**

datum

# The Datum Platform

## Datum Storage

Datum Storage is a highly secure key-value store - similar to AWS S3 or Azure Blob Storage - designed for mission critical data storage. Developers can use Datum Storage to securely store and retrieve objects of up to 2 gigabytes, such as structured data, files, or documents. Stored data is automatically replicated on two or more storage nodes, and replication levels can be configured to meet business requirements on a per-object basis. Encryption ensures that individual storage nodes have no knowledge of the data they are storing, ensuring security and integrity of data.

## Datum Exchange

The Datum Data Exchange Protocol (Datum Exchange) allows secure party-to-party sharing and transfer of data while enforcing access control based on business requirements. Data can be shared for free or with monetary compensation and enables companies to run internal data marketplaces to serve subsidiaries, business units, or even external customers. Each transaction is immutably recorded ensuring compliance with all applicable regulations.

## Datum Encryption

Datum is well suited for mission-critical data storage. All data is encrypted using a military grade AES-256 block cipher in combination with 256-bit elliptic curve cryptography, equivalent in computational complexity to a 3072-bit RSA key. Datum ensures permissioned access through a distributed PKI (Public Key Infrastructure). Data is encrypted at the source, remains encrypted during transmission and can be securely shared with receiving parties without requiring out-of-band secret key sharing. Encryption keys are controlled by the data source and data consumers and never leave the device.

## Datum Identity

A Datum Identity - and the Datum ID mobile app - is an optional add-on to extend data ownership to individuals and organizations. The Datum Identity enables secure universal login, multi-factor authentication, and claims verification backed by a digital identity anchored to an immutable blockchain layer. Users can digitally sign claims to make statements which are tamper-proof and cryptographically verifiable. The Datum Identity can be used to augment traditional login mechanisms in centralized or federated login systems, or be used on its own as self-sovereign digital identity under the full control of the subject.

## Datum Consent

Datum Consent gives companies a full suite of tools to acquire consent from data subjects, attach that consent permanently to the data, and then exchange data with one another with that consent intact.

## Private Enterprise Deployments

The complete Datum infrastructure is deployable as private blockchain in the cloud or on premises. The Datum distributed ledger immutably tracks incoming and outgoing data from the key value store ensuring all access to data is tracked and access permissions are governed according to your business requirements.

# Datum Storage vs. Traditional Data Stores

| | Datum | AWS S3 | Azure Blob Storage |
|---|---|---|---|
| Automatic Replication of entire Storage Bucket | Yes | Yes | Yes |
| *Automatic* Geographical Replication according to business rules on a per object basis | Yes | No | No |
| Client-Side encryption of each individual object | Yes | No | No |
| Server-Side encryption | Yes | Yes | Yes |
| *Automatic* Object Versioning | Yes | Yes | No |
| Storage Provider does not have knowledge of data | Yes | No | No |
| Access Log | Yes | Yes | Yes |
| DLT based access log | Yes | No | No |
| Access Control | Yes | Yes | Yes |
| DLT based Access Control | Yes | No | No |
| REST API | Yes | Yes | Yes |
| Javascript SDK | Yes | Yes | Yes |
| AWS-SDK compatible | Yes | Yes | No |
| Automatic shortest path routing | Coming Soon | No | No |
| Built in Monitoring | Yes | Yes | Yes |
| Add Object | Yes | Yes | Yes |
| Update Object | Yes | Yes | Yes |
| Remove Object | Yes | Yes | Yes |
| Public Sharing of Objects | No | Yes | Yes |
| DLT Permissioned Private Sharing based on ACLs and business logic per object | Yes | No | No |
| Optional Metadata per object | Yes | Yes | Yes |

# Use Cases

## Consent Tracking of Personal User Data

With the EU introduction of the General Data Protection Regulation (GDPR) and many jurisdictions following suit, it is important for companies to establish clear parameters and process for handling of personal user data. Point the Datum Consent toolchain at your internal data warehouse - or upload data directly to Datum Storage, our secure storage offering. Datum Consent creates an intermediary layer where all personal user data flows are captured, documented and permissioned. Ensuring compliance with GDPR and other data protection regulations.

## Secure Storage of Highly Sensitive Data

Storage of sensitive financial or medical personal data, such as passport copies for KYC purposes or medical history of individuals, requires careful planning around data storage security. The Datum Data Store provides a secure, out of the box data store that can satisfy strict data security requirements, many of which are enforced on a technical level rather than simply relying on flawless administration.

## Trusted Object Store across Multiple Untrusted Parties

Datum can act as a trusted object store, federating data storage of multiple, potentially untrusted parties. An example is a data store for wire transfer account information used in real estate escrow processes, real estate wire transfer fraud is rampant with over $1B attempted yearly in the US alone. Various parties such as the seller, buyers, lawyers, agents, title insurance companies and land registries need access to a trusted source of information for critical data. Datum provides a secure data store with integrity guarantees including signature verification of participants, verifiable independently by all parties.