

# INTERNATIONAL DATA SPACES ASSOCIATION

The background of the cover is a complex, abstract network of glowing lines in various colors (green, yellow, orange, blue, purple) against a dark background, suggesting a data ecosystem or network.

## INTERNATIONAL DATA SPACES IDS – A STANDARD FOR DATA SOVEREIGNTY AND AN INDISPENSABLE ELEMENT OF DATA ECOSYSTEMS

*Version 1.0 | September 2019*



## IDS – A STANDARD FOR DATA SOVEREIGNTY AND AN INDISPENSABLE ELEMENT OF DATA ECOSYSTEMS

**Data sovereignty: Assigning binding usage restrictions to data; establishing a concept and components for a secure and trusted data infrastructure.**

The International Data Spaces Association (IDSA) has defined a reference architecture and a formal standard to be used for creating and operating virtual data spaces. The IDS Architecture is based on commonly accepted data governance models facilitating secure exchange and easy linkage of data within business ecosystems.

The IDS Architecture ensures digital sovereignty for data owners making data available for being exchanged or shared. It thereby constitutes the basis for developing and offering smart services and for establishing innovative business processes.

The IDS initiative aims at creating a secure and trusted data space, in which companies of any size and from any industry can manage their data assets in a sovereign fashion. It addresses companies and other organizations from across Europe and beyond. IDSA already counts over one-hundred member organizations from twenty countries.

**Data** is the raw material for innovation. This is particularly true for three major areas that are of paramount importance in today's digitalized world: artificial intelligence (AI), the internet of things (IoT), and big data. For data to unfold its full potential, it must be made available in cross-company, cross-industry business ecosystems.

**Data value chains** range from capturing data by means of sensors to preprocessing, storing, and transferring data to eventually data analysis, data processing, and data usage. The existence of data value chains is a

necessary precondition for achieving innovation within business ecosystems.

**Data sovereignty** in IDS presupposes meta-data attached to data, which unambiguously defines data usage restrictions at each level of the data value chain. Enforcing data sovereignty requires an appropriate technical infrastructure that facilitates contractual agreements on the use of data, such as allowing (or disallowing) the processing, linkage or analysis of data by data users, or allowing (or disallowing) third parties access to data. If need be, data sovereignty is ensured also within third parties' digital infrastructures (e.g. networks, clouds, or software components).

**IDS Connector – the gateway software component of a technology made in Europe**

To incentivize the exchange of data among organizations and individuals across Europe, a technology "made in Europe" is needed. This technology must ensure data sovereignty across different industries and on a non-competitive basis by means of appropriate digital infrastructure components and a standard, interoperable format.

The IDS initiative has developed a software architecture that ensures data sovereignty by facilitating secure exchange of data between trusted parties. Certified users are granted access to the data ecosystem, in which they can attach usage restriction policies to their data before they make it available to other users. This is made pos-



sible by a dedicated gateway software component, the IDS Connector, which can be installed on a server, in a cloud, on an IoT device, and on a smartphone.

This way, data is generated decentrally, before it can be exchanged with the help of IDS technology, stored in any kind of cloud (public, private, etc.), and processed in line with data usage policies specified. The IDS Connector uses special container technology ensuring “trusted execution”; i.e. data inside the container is always protected against unauthorized access and manipulation, and can be used only as agreed upon by the parties involved.

### **Using trusted infrastructures to enforce data sovereignty**

Trusted infrastructures constitute the basis for ensuring data sovereignty in the first place. Such infrastructures must be equipped with a number of mutually adjusted operational components (e.g. identity management or dynamic trust management) and allow for unambiguous digital identities. If either of these two preconditions is missing, data sovereignty cannot be enforced. It is these components and identities, together

with additional IDS features (such as a broker service provider or functions for data quality assessment), that make a data ecosystem based on data sovereignty valuable for its users. Therefore, the overall goal of IDSA is to design and develop a secure and trusted digital infrastructure that relies on basic European values.

### **Digital platforms as data ecosystems**

Whether we speak of business, politics, the media, or society – digital platforms have become an indispensable element in today’s digitalized world. These platforms provide access to products, services, digital content, information, and data for everybody. When it comes to bringing supply and demand together as efficiently as possible, digital platforms clearly outmatch traditional business models. They have evolved from technical instruments to complex ecosystems. Digital platforms can create new markets, and stimulate existing ones. Across highly fragmented markets, they can bring together people or companies who otherwise would never have gotten in contact with one another. In short: Digital platforms bear an enormous potential and countless opportunities.

**Digital platforms; applications in the fields of AI, IoT, or big data; projects such as GAIA-X or AI4EU – all these endeavors and application areas cannot be conceived of without IDS. IDS will significantly contribute to the success of these endeavors and application areas. Being an open standard for facilitating secure and trusted data exchange that is guided by the principles of data sovereignty, IDS should be integrated as an inherent component in future architecture models of the data economy.**

## CONTACT

---


Head Office

INTERNATIONAL DATA SPACES ASSOCIATION

Emil-Figge-Str. 80  
44227 Dortmund | Germany

phone: +49 231 70096 501  
mail: [info@internationaldataspaces.org](mailto:info@internationaldataspaces.org)

[WWW.INTERNATIONALDATASPACE.S.ORG](http://WWW.INTERNATIONALDATASPACE.S.ORG)

 [@ids\\_association](https://twitter.com/ids_association)

 [international-data-spaces-association](https://www.linkedin.com/company/international-data-spaces-association)