INTERNATIONAL DATA SPACES ASSOCIATION

Position Paper | Version 1.0 | December 2019

GDPR Related Requirements and Recommendations for the IDS Reference Architecture Model

● Position Paper of members of the IDS Association
○ Position Paper of bodies of the IDS Association
○ Position Paper of the IDS Association
○ White Paper of the IDS Association

Fraunhofer

Publisher

International Data Spaces Association

Anna-Louisa-Karsch-Str. 2

10178 Berlin

Germany

Editor

Sebastian Steinbuss

International Data Spaces Association

Cite as

Steinbuss S. et al. (2019): GDPR Related Requirements and Recommendations for the IDS Reference Architecture Model. International Data Spaces Association. https://doi.org/10.5281/zenodo.5675903

Contributing Projects

https://www.fraunhofer.de/en/research/lighthouse-projects-fraunhofer-initiatives/industrial-data-space.html

Authors & Contributors:

Benjamin Heitmann, Fraunhofer FIT

Dr.-Ing. Erik Krempel, Fraunhofer IOSB

Michael Ochs, Fraunhofer IESE

Dustin Schutzeichel, Fraunhofer FIT

Executive Summary

GDPR compliance of an organization is only fulfilled by the implementation of both appropriate technical measures and appropriate organizational measures.

By participation of an organization in an IDS based ecosystem, the software which implements the IDS RAM can provide the technical measures.

However, the responsibility and accountability with respect to GDPR compliance is on the part of the organization participating in the IDS ecosystem. This organization has to implement adequate organizational measures for the protection of personal data. This set of measures may be set up based on a risk assessment of personal data and personal data processing and - if the risk level exceeds certain thresholds - a data protection impact assessment.

Consequently, the organizations participating and their data processing within an IDS-based ecosystem have to be considered for GDPR compliance (see section 4.1 in D2 – Analysis of the GDPR along the Use Cases).

Therefore, it cannot be said in general that “the IDS” is GDPR-compliant. Instead, the role of "the IDS" towards GDPR compliance should be in supporting the organizations participating in an IDS-based ecosystem through the implementation of technical measures and by giving advice about organizational measures. As a result, an IDS participant is enabled to set up GDPR-compliant processing and transfer of personal data within the scope of the IDS technology and features.

We recommend investigating the inclusion of the identified technical and organizational measures (a potential subset of which is advised in this document) in the IDS certification process of an organization.

For all identified technical requirements, we list priorities and give our recommendations with regard to GDPR compliance in concrete application scenarios.

In addition, we have identified four requirements, which could represent unique selling points (USP) of the IDS towards the goal of achieving a higher level of data control and therefore allow business cases so far not possible with existing technology.

Table of Contents

Executive Summary 3

Table of Contents 4

1 Introduction 5

2 Technical Measures for the IDS Reference Architecture Model to Support GDPR Compliance 6

2.1 Alignment of Epics and Requirements 6

2.1.1 Processing 6

2.1.2 Storage 8

2.1.3 Access Control, Usage Control & Security 8

2.1.4 Metadata 9

2.2 Technical Requirements 9

3 Organizational Measures for the IDS Ecosystem to Support GDPR Compliance 25

3.1 Alignment of Epics and Requirements 25

3.1.1 Processing 25

3.1.2 Access Control, Usage Control & Security 25

3.1.3 Metadata 25

3.2 Organizational Requirements 26

4 Categorization and Prioritization of the Technical Requirements 37

1a) Must Have 38

1b) Continue Implementing 38

2) Keep and Carry On 39

3) Recommended 39

4) Uncritical 41

5 Unique Selling Points 43

6 Realization of Organizational Requirements 44

7 Summary and Next Steps: Towards Compliance of the IDS with the GDPR 47

.... 1

1 Introduction

This paper aims at a derivation of requirements for the IDS reference architecture model (IDS RAM) in order to support the compliance with the General Data Protection Regulation (GDPR).

The fundament for this is the identification, detailed documentation and analysis of the use cases in the International Data Space, which involve the processing of personal data, thus being relevant for the GDPR. For the description of the use cases see the document D1 – Identification and Documentation of Relevant Use Cases[1]. Further information on the analysis and the GDPR compliance can be found in D2 - Analysis of the GDPR along the Use Cases[2].

First, a summary of necessary functionalities for the IDS is given that originate from the analysis of our use cases presented in D2 – Analysis of the GDPR along the Use Cases[3]. Based on the identified functionalities, more fine-grained requirements are formulated. Finally, we elaborate a categorization and prioritization of the requirements serving as our recommendation for the future work of the IDS initiative with respect to GDPR compliance. We argue to what extent the IDS ecosystem can contribute to GDPR compliance of organizations processing and sharing personal data - and which aspects are out of scope of the IDS.

[1] https://industrialdataspace.jiveon.com/docs/DOC-2953
[2] https://industrialdataspace.jiveon.com/docs/DOC-2954
[3] https://industrialdataspace.jiveon.com/docs/DOC-2953

2 Technical Measures for the IDS Reference Architecture Model to Support GDPR Compliance

This section presents all necessary technical measures for IDS we were able to identify in the considered use cases. We collect these in a scenario specific context and in the next step try to break them down into generic requirements. In the following, we also align the derived epics from the document D2 – Analysis of the GDPR along the Use Cases[4] with the categories of measures. For further information, see section 4 in D2 – Analysis of the GDPR along the Use Cases[5].

2.1 Alignment of Epics and Requirements

2.1.1 Processing

Technical measures from the use cases that involve the processing of data, including the data transfer between IDS connectors.

- **E-1:** Usage of a category-based query interface to satisfy requirements and principles of purpose limitation and data minimization.
  - Req_DataSemantics
  - Req_DomainSpecificVocabulary
  - Req_DataLabeling
  - Req_CategoryBasedQueryInterface
- **E-3:** Data filtering and/or aggregation capabilities can be installed on the outgoing interface of the data provider's IDS connector and/or on the ingoing interface of the data consumer's IDS connector, thus satisfying requirements and principles of purpose limitation and data minimization.
  - Req_DataSemantics
  - Req_Aggregation
  - Req_RemoteAttestation
- **E-6:** Transfer of data between source and destination is encrypted.
  - Req_DataTransferEncryption
- **E-8:** Transfer of data is based on an access token with limit validity (duration for the specific purpose in the use case could be less than 12h).
  - Req_DataAccessRestrictions

[4] https://industrialdataspace.jiveon.com/docs/DOC-2953
[5] https://industrialdataspace.jiveon.com/docs/DOC-2954

- **E-9:** IDS connectors are capable to anonymize personal data "on the fly" at transfer/transmission execution time if a policy, processing purpose or user consent tells so.
  - Req_DataSemantics
  - Req_Anonymization
  - Req_UsagePolicyNegotiation
  - Req_UsagePolicyEnforcement
  - Req_RemoteAttestation
- **E-10**: IDS connectors are capable to remove any attribute of information (e.g. stemming from video/audio meta data) "on the fly" from data stream or object at transfer/transmission execution time if a data policy, usage agreement, processing purpose or user consent tells so.
  - Req_DataSemantics
  - Req_Anonymization
  - Req_UsagePolicyNegotiation
  - Req_UsagePolicyEnforcement
  - Req_RemoteAttestation
- **E-11:** For auditing purposes, the processing activities in the IDS connector are recorded, including the purpose of processing, the kind of processing operation, the kind of processed data, information about possible data storage (location and duration), the provider, the consumer, the service and possible recipients of data. Such an audit log represents a key enabler for the information rights of data subjects, who are empowered to request detailed information about how their data are processed and to verify whether their data have actually been processed in accordance to the established consent. Data controllers can effectively demonstrate compliance with the GDPR (and other data protection regulations) towards supervisory authorities ('accountability principle', cf. Art. 5 (2) GDPR and 'notification of a personal data breach to the supervisory authority', cf. Art. 33 GDPR).
- (**E-2:** Epic E-2 has been merged with E-11 due to the conceptional intersection of both epics.)
  - Req_DataSemantics
  - Req_DomainSpecificVocabulary
  - Req_DataLabeling
  - Req_AuditLog
  - (Req_ConsentManagement_Tech)
- **E-20:** The data subject rights according to Art. 15 - 22 GDPR are supported by technical measures. This includes technical measures to provide a basis to deliver transparent information to the GDPR-related processes towards the data subject about the

personal data processing (Art. 12 - 15), for data portability (Art. 15 (3), Art. 20), for the correction of inaccurate personal data (Art. 16, Art. 19), for the erasure of personal data (Art. 17, Art. 19), for the restriction of personal data processing (Art. 18) and for the objection against personal data processing (Art. 21).

  - Req_DataSubjectRights_Tech
  - Req_DataSemantics
  - Req_DomainSpecificVocabulary
  - Req_DataLabeling
  - Req_AuditLog
  - Req_ConsentManagement_Tech

2.1.2 Storage

Technical measures from the use cases that involve storage and management of data, which is a special category of data processing.

- **E-7:** On the fly encryption of data while transfer to persistence layer
  - Req_DataTransferEncryption
- **E-12:** The data storage is encrypted.
  - Req_DataStorageEncryption

2.1.3 Access Control, Usage Control & Security

Technical measures from the use cases that involve management of access or usage rights and other elements of IT-security.

- **E-13:** 4-eye/peer login capability before data access is granted, anonymization capabilities if 2-eye login only is executed
  - Req_FourEyeLogin_Tech
- **E-14:** IDS connectors are capable to distinguish between 4/2-eye access and act according to the related active 4/2-eye context.
  - Req_FourEyeLogin_Tech

- **E-21:** The notification of a personal data breach to the supervisory authorities and the communication of a personal data breach to the data subject according to Art. 33 and 34 GDPR are technically supported.
    - Req_DataBreachCommunication_Tech
    - Req_DataSemantics
    - Req_DomainSpecificVocabulary
    - Req_DataLabeling
    - Req_AuditLog

2.1.4 Metadata

One of the core concepts of IDS is the availability of metadata. This enables data owners to describe their data and therefore make it available for data processors. Data processors can search existing metadata to find the necessary data for their application.

- **E-4:** Knowledge and specification of the format/schema of the transferred data sets are available in order to automatically filter and/or aggregate data.
    - Req_DataSemantics
    - Req_DomainSpecificVocabulary
    - Req_DataLabeling
- **E-5:** A catalog, vocabulary or list of codes of bank transaction categories is available, e.g. provided by a service in the Open API (PSD2) interface or by an artificial intelligence.
    - Req_DomainSpecificVocabulary

2.2 Technical Requirements

In the following, more fine-grained requirements for the IDS reference architecture model (IDS RAM) with respect to technical measures are denoted. These serve as a support for compliance with the obligations of data controllers and the rights of data subjects according to the GDPR. For more detailed information on the legal concepts from the GDPR, see section 2 in D2 – Analysis of the GDPR along the Use Cases[6].

[6] https://industrialdataspace.jiveon.com/docs/DOC-2954

ID	Req_DataLabeling
Generic Requirement	Label data to define its secrecy level, including storage time, access restrictions. Data labeling is used to define what can/should happen to data.
Measurement **(How to measure whether the requirement is met?)**	Does a way to annotate data exist?
Fulfilled by the IDS RAM? **(Yes, No)**	No - there is only a reference to IEC 62443 security levels. The extent of required labeling has to be defined.
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	No Internal guidelines specific to categories of data, storage/usage time, etc. are required by Art. 47 GDPR. Moreover, Art. 30 GDPR requires records of processing activities. This requirement offers an electronic and automatically processable labeling of data covering relevant aspects of Art. 5, 6, 9, 25 and 32 GDPR as a potential part of electronically accessible and processable records of processing activities.

ID	Req_DomainSpecificVocabulary
Generic Requirement	Req_DataLabeling enables a system to describe how data can be processed. To enable this, a domain specific vocabulary is needed. In addition, vocabularies are necessary to denote GDPR-related aspects, such as the *purpose* of data processing (e.g. PROFILING, MEDICAL_TREATMENT, ...) and the kind of data processing operation performed on the personal data (e.g. ANONYMIZE, STORE, TRANSFER, ...). For the banking use cases, there is also a need for domain-specific vocabularies in order to *categorize* bank transaction data (e.g. FOOD, INSURANCE, TRANSPORT, ...), thus allowing for data aggregations and purpose limitation.
Measurement **(How to measure whether the requirement is met?)**	Is domain specific language broken down into technical requirements where applicable? Is corresponding vocabulary provided and documented?
Fulfilled by the IDS RAM? **(Yes, No)**	No, depends on Req_DataLabeling There are no ongoing activities regarding this requirement.

Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	No Supports Art. 6 vs. Art. 9 concerning the types of personal data.

ID	Req_DataSemantics
Generic Requirement	Analogously to requirement Req_DataLabeling, knowledge about the semantics of data processed by IDS connectors is required. For example, it may be required to know about which kind of attributes in a certain data packet, e.g. a JSON-conformable document, is personal data. Such knowledge about data semantics allows software components, e.g. Data Apps running in the IDS connector, to remove/aggregate/anonymize certain data attributes "on the fly". A removal/aggregation/anonymization of personal data attributes may be necessary in order to comply with deployed usage control polices or binding laws, for example.
Measurement **(How to measure whether the requirement is met?)**	Is the data processed by IDS connectors annotated with machine-readable semantic information? Does the semantic information allow for filtering/aggregation/anonymization operations?
Fulfilled by the IDS RAM? **(Yes, No)**	No - the IDS Information Model allows for defining segments of structured content, though it has not yet been applied to annotate GDPR relevant "parts" of data.
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	No Supports distinguishing between types of data (personal/non personal), c.f. Art. 4 (1).

ID	Req_ProcessingCertification
Generic Requirement	All data is processed according to access/usage control policies. Apps that access sensitive data, i.e. data with a classification level or sensitive personal data, can be certified. This requirement technically supports the organizational requirement Req_ParticipantCertification.
Measurement **(How to measure whether the requirement is met?)**	Is there a certification process for participants verifying their trustworthiness? Is the processing of sensitive information such as personal data, restricted to certified participants in an IDS ecosystem?
Fulfilled by the IDS RAM? **(Yes, No)**	Yes. There is a formal process of *participant* and *connector* certification defined. *Data App* certification is subject of future development.
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	No See Art. 42 GDPR, while the IDS certification is not considered to be done by supervisory authorities.

ID	Req_RemoteAttestation
Generic Requirement	Remote attestation allows a data owner decide if a system is trustworthy / in a certain configuration before sending data to it. This is especially important if data with a high level of sensitivity is to be transmitted and the owner must ensure that the receiver acts according to some regulation.
Measurement **(How to measure whether the requirement is met?)**	Can a data owner verify a data receiver before giving him data?
Fulfilled by the IDS RAM? **(Yes, No)**	Yes. Defined as part of the IDS Secure Communication Protocol (IDSCP). Implementation status to be clarified.
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	No Implicit connection with Art. 20 (1) + (2) based on Art. 6 (1) a+b and/or Art. 9 (2) b (supports data sovereignty "on demand").

ID	Req_Anonymization
Generic Requirement	IDS connectors needs to be capable to anonymize data packets containing personal data attributes, e.g. a name, an address, another identification number revealing the identity of an individual. The anonymization may take place "on-the-fly" at the outgoing interface of IDS connectors, such that no personal data effectively leave the connector. Alternatively, it may be done at the incoming interface of an IDS connector. Thus, the anonymization serves as an instrument for data minimization and avoids the processing of personal data at all, where possible. For this purpose, a data app for anonymization purposes may be used, e.g. to remove/filter personal data related attributes from data packets. Appropriate information about data semantics are required, as stated in Req_DataSemantics. Assuming a generic Anonymization App some *configuration* of the anonymization process on particular type of data may be required.
Measurement **(How to measure whether the requirement is met?)**	Is it possible to anonymize data packets processed in an IDS ecosystem, i.e. are IDS connectors capable to remove personal data attributes?
Fulfilled by the IDS RAM? **(Yes, No)**	No (No ongoing activities regarding this requirement are known.)
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	No Anonymization is the instrument to leave the GDPR scope. If data are anonymized before e.g. transferring them to another IDS participant, the GDPR does not apply anymore. See Recital 26 and Art. 11 GDPR.

ID	Req_Aggregation
Generic Requirement	Analogously to Req_Anonymization, capabilities to aggregate attributes from data packets are required. This results in purpose limitation and data minimization.
Measurement **(How to measure whether the requirement is met?)**	Is it possible to aggregate data packets processed in an IDS ecosystem, i.e. are IDS connectors capable to aggregate personal data attributes?
Fulfilled by the IDS RAM? **(Yes, No)**	No (No ongoing activities regarding this requirement are known.)
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	No Aggregation or pooling of data represents a transfer and storage of data potentially not conforming to the original purpose and lawfulness of processing given at data collection time and has to be treated with care, c.f. Art. 6 (4).

ID	Req_CategoryBasedQueryInterface
Generic Requirement	Analogously to Req_Aggregation, a category-based query interface to satisfy requirements and principles of purpose limitation and data minimization is necessary.
Measurement **(How to measure whether the requirement is met?)**	Is it possible for IDS connectors to query/offer data of a certain category only?
Fulfilled by the IDS RAM? **(Yes, No)**	No (No ongoing activities regarding this requirement are known.)
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	No Not required, but a desirable method for supporting data minimization and limitation.

ID	Req_UsagePolicyNegotiation
Generic Requirement	Usage policies between data provider and data consumer can be (dynamically) negotiated. The usage policies encode the rules how the data are allowed to be processed. Such usage policies may involve temporal restrictions, e.g. the

	data can only be used for 3 days, or purpose limitations, e.g. the data can only be used for medical treatment purposes.
Measurement **(How to measure whether the requirement is met?)**	Does a way to represent usage policies exist? Can usage policies be negotiated between data provider and data consumer?
Fulfilled by the IDS RAM? **(Yes, No)**	Partially - terms of usage policy language based on ODRL are being defined. The negotiation process is subject of ongoing FDS project T14.
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	No Not required, but a desirable method for purpose limitation. This requirement support automated data transfer between organization, e.g. in case, the lawfulness of processing founds on a contract between the data subject and the controller and the second organization supports the controller in contract fulfilment and is in need of contract-relevant personal data.

ID	Req_UsagePolicyEnforcement
Generic Requirement	The technical enforcement of negotiated usage policies is implemented.
Measurement **(How to measure whether the requirement is met?)**	Are the negotiated usage policies enforced on a technical basis, i.e. are the IDS connectors capable to enforce the usage policies?
Fulfilled by the IDS RAM? **(Yes, No)**	Partially - part of IDSPlus AP6/AP7 activities. (Check whether the current enforcement capabilities match the needs)
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	Yes Supports Art. 6 (1) and/or Art. 9 (2) and/or Art. 20 (2) in connection with Art. 25 and Art. 32 GDPR.

ID	Req_DataTransferEncryption
Generic Requirement	The data transfer between data provider and data consumer is encrypted.

Measurement **(How to measure whether the requirement is met?)**	Is the data transfer between data provider and data consumer in an IDS ecosystem protected against man-in-the-middle and eavesdropping attacks?
Fulfilled by the IDS RAM? **(Yes, No)**	Yes (TLS used for data transfer between IDS trusted connectors)
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	Yes See Art. 25 and Art. 32 GDPR.

ID	Req_DataStorageEncryption
Generic Requirement	Not only the data transfers between IDS connectors have to be encrypted according to Req_DataTransferEncryption, but also the encryption of the data storage is desired. According to the specification of the IDS RAM, the data processing within an IDS-based ecosystem typically involves the processing within the technical scope of the IDS connector operated by the data provider. In this respect, data are processed along a route, i.e. a sequence of IDS data apps or other internal processing components performing data manipulation operations. Considering the IDS as an enabler for data sharing use cases across organizational boundaries, the processing usually involves the transmission of data to another organization. Conforming to the IDS terminology, the organization receiving the data acts as the data consumer. Technically, data are received by the connector operated by the data consumer, which performs certain data-related operations as well. In this context, we assume the existence of business use cases in an IDS-based ecosystem, in which the data processing does not stop within the boundary of the data consumer's IDS connector. Instead, it is assumed that data are persisted in a data sink on the site of the data consumer. Depending on a risk and data protection impact assessment according to Art. 35 GDPR, it may be required or at least desirable to store the data in an encrypted manner. In case of personal data according to Art. 4 (1) and in particular, special categories of personal data as to Art. 9 (1) GDPR, it is advisable to ensure an encrypted storage of data.

	On that front, the IDS could technically support this possible requirement. For example, it could provide technical instruments ensuring an encrypted delivery of data to the data storage layer. IDS connectors could enforce data to be encrypted before leaving the IDS connector for storage purposes. In addition, the certification process proposed by the IDS RAM could include the assessment of the technical and organizational measures regarding the security of data storage. In the certification of an organization aiming at the participation in the IDS ecosystem, it could be examined whether the data storage layer attached to the IDS connector operated by that organization uses encryption, e.g. hardware-based full disk encryption. The resulting certificate could transparently state whether the IDS participant stores data in an encrypted way, thus increasing its level of trustworthiness.
Measurement	Are personal data, which are processed in an IDS ecosystem, stored in an encrypted data store only?
Fulfilled by the IDS RAM?	No (No ongoing activities regarding this requirement are known.)
Criticality for IDS with respect to GDPR Compliance	No Depending on a risk and data protection impact assessment according to Art. 35, the encrypted storage of personal data may be desirable. See also Art. 25 and Art. 32 GDPR.

ID	Req_ConsentManagement_Tech
Generic Requirement	The management of data subjects' consent is required, which can serve as legitimation for law-compliant personal data processing. In particular, this involves: Storage of consent information, e.g. data subject, date of consent, scope of the consent Possibility for data subjects to withdraw/change the previously provided consent This requirement is associated with a technical realization of the consent management, while Req_Con-

	sentManagement_Org focuses on the underlying organizational measures required as part of the consent management.
Measurement **(How to measure whether the requirement is met?)**	As soon as the personal data processing is based on the data subject's consent, does a consent management solution exist?
Fulfilled by the IDS RAM? **(Yes, No)**	No (No ongoing activities regarding this requirement are known.)
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	No Consent management as an organizational measure (see Req_ConsentManagement_Org) is required in case that the lawfulness of the personal data processing is based on the data subject's consent. Nevertheless, an implementation of consent management on the technical level is not enforced by the GDPR. See Art. 6 (1) lit. a, Art. 7, Art. 8, Art. 9 (2) lit. b GDPR.
ID	Req_AuditLog
Generic Requirement	A GDPR-compliant audit log of processing operations on personal data performed in the IDS ecosystem(s) is required. This serves as a support for data subjects' transparency rights and a foundation for (automatic) compliance verification whether IDS participants actually process personal data in accordance with the obtained consent.
Measurement **(How to measure whether the requirement is met?)**	Does a verifiable record about the processing activities related to personal data exist?
Fulfilled by the IDS RAM? **(Yes, No)**	No (The term 'audit log' is used in the IDS RAM, but it is questionable whether this corresponds to our needs with respect to compliance with the GDPR. The data provenance tracking approach envisioned in the current IDS RAM 3.0 is related to this requirement. However, it is also unclear whether this matches the requirements of a GDPR-compliant audit log. Furthermore, there is no concrete implementation yet.)

Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	No In general, an audit log of personal data processing activities in the IDS ecosystem supports the transparency rights towards data subjects (Art. 12 - 15) and supervisory authorities (Art. 30 (4), Art. 31, Art. 33). The audit log is not a strict requirement stated by the GDPR. However, it can also be derived from Art. 33 GDPR. Especially Art. 33 (3) lit. a requires the categories of data concerned by a breach of data protection and the number of affected data subjects. Moreover, it simplifies fulfilling the requirements of Art. 33 (4) and Art. 33 (5) GDPR.

ID	Req_DataAccessRestrictions
Generic Requirement	Restrictions for the data access are required, e.g. time-based limitation (→ access token with limited validity). The definition of access restrictions is aligned with the usage policy framework, since access is considered a (transient) type of usage. This requirement is also related to the encryption requirements Req_DataTransferEncryption and Req_DataStorageEncryption aiming at the security of personal data during transmission between connectors and at rest in data sinks. Thus, they provide a technical support of access control.
Measurement **(How to measure whether the requirement is met?)**	Can the data access be temporarily restricted?
Fulfilled by the IDS RAM? **(Yes, No)**	Partially - as part of the usage policy framework.
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	Yes Data access restriction may cover internal, e.g. by services or by employees, and external access. Art. 25 and Art. 32 GDPR require adequate technical and organizational measures to support the defined protection objectives.

ID	Req_FourEyeLogin_Tech
Generic Requirement	4-eye/peer login capability before data access is granted - or anonymization capabilities if 2-eye login only is executed IDS connectors are capable to distinguish between 4/2-eye access and act according to the related active 4/2-eye context.
Measurement **(How to measure whether the requirement is met?)**	Do 4-eye/peer login capabilities exist to restrict the access to sensitive data?
Fulfilled by the IDS RAM? **(Yes, No)**	No (No ongoing activities regarding this requirement are known.)

Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	No Not required by GDPR explicitly, but is within the scope of potential organizational measures for integrity and privacy of personal data, e.g. in case of video surveillance. The technical capability of a 4-eye login would support the corresponding organizational measure. The implementation cost of such a mechanism appear too acceptable.

ID	Req_ContextRelatedSystemDeactivation_Tech
Generic Requirement	Depending on a certain context, such as a demonstration, the system that handles personal data is shut down / deactivated by the organization. Otherwise, the personal data may be involuntarily shown to non-authorized persons, e.g. the attendees of a system demonstration. The requirement may be conceptualized as a context-aware usage policy demanding appropriate policy definition and handling of "current context" by the related component(s) (PIP attributes).
Measurement **(How to measure whether the requirement is met?)**	Is the IDS connector context-aware? Is the usage control framework implemented in the IDS connector capable to handle the current system context and allow/deny data flows based on context-related usage policies?
Fulfilled by the IDS RAM? **(Yes, No)**	Partially, as part of the usage policy framework.
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	No It is not required, but desirable.

ID	Req_EmergencyAccessRestriction_Tech
Generic Requirement	Human access to production data is restricted to emergencies only, e.g. a production stop or similar failures needing for a hot fix. Otherwise, humans do not have access to production data at all. Same relation to "context aware" usage policies applies as with Req_ContextRelatedSystemDeactivation_Tech.
Measurement **(How to measure whether the requirement is met?)**	Is the IDS connector context-aware? Is the usage control framework implemented in the IDS connector capable to handle the current system context and allow/deny data flows based on context-related usage policies?
Fulfilled by the IDS RAM? **(Yes, No)**	Partially, as part of the usage policy framework.
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	No, but part of other regulations, e.g. Bafin regulations for financial services. It is not required, but desirable.

ID	Req_DataSubjectRights_Tech
Generic Requirement	While the data subject rights according to Art. 15 - 22 GDPR are primarily considered as organizational measures, a technical support to facilitate the realization of the data subject's rights is desirable. This includes technical mechanisms for transparent information about the personal data processing (Art. 12 - 15), for data portability (Art. 15 (3), Art. 20), for the correction of inaccurate personal data (Art. 16, Art. 19), for the erasure of personal data (Art. 17, Art. 19), for the restriction of personal data processing (Art. 18) and for the objection against personal data processing (Art. 21). This technical requirement is associated with the following organizational requirements related to the stated data subject rights: Req_DataSubjectRights_TransparentInformation Req_DataSubjectRights_DataPortability Req_DataSubjectRights_DataCorrection Req_DataSubjectRights_DataErasure Req_DataSubjectRights_ProcessingRestriction Req_DataSubjectRights_ProcessingObjection
Measurement **(How to measure whether the requirement is met?)**	Are technical instruments in place facilitating the exercise of the data subject rights according to Art. 15 - 22 GDPR?
Fulfilled by the IDS RAM? **(Yes, No)**	No
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	No The technical implementation is not required, but desirable.

ID	Req_DataBreachCommunication_Tech
Generic Requirement	In the case of a personal data breach, the data controller has to inform both the supervisory authority (Art. 33) and the affected data subject (Art. 34). The data controller has to describe the likely consequences of the data breach and document the measures taken or proposed to be taken. This technical requirement is associated with the following organizational requirements related to the stated communication of personal data breaches: Req_DataBreachCommunication_SupervisoryAuthority Req_DataBreachCommunication_DataSubject
Measurement **(How to measure whether the requirement is met?)**	Are technical instruments in place supporting the communication of personal data breaches towards the supervisory authorities and the data subjects?
Fulfilled by the IDS RAM? **(Yes, No)**	No
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	No The technical implementation is not required, but desirable.

3 Organizational Measures for the IDS Ecosystem to Support GDPR Compliance

This section presents all necessary organizational measures for IDS we were able to identify in the considered use cases. We collect these in a scenario specific context and in the next step try to break them down into generic requirements. In the following, we also align the derived epics from document D2 - Analysis of the GDPR along the Use Cases[7] with the categories of measures. For further information, see section 4 in D2 – Analysis of the GDPR along the Use Cases[8].

3.1 Alignment of Epics and Requirements

3.1.1 Processing

Organizational measures from the use cases related to the processing of data.

- **E-17:** 4-eye/peer principle when analyzing persisted data with human involvement
  - Req_FourEyeLogin_Org
- **E-18:** Deactivation of a system with critical data (e.g. video data in the surveillance use case) during a demonstration. (Nowadays this is done manually, it could be an information provided by an PIP and the enforced in the system)
  - Req_ContextRelatedSystemDeactivation
- **E-19:** A login/access to sensitive personal data is only granted to relevant personnel (by role and data resolution)
  - Req_AccessControl

3.1.2 Access Control, Usage Control & Security

Organizational measures from the use cases that involve management of access or usage rights and other elements of IT-security.

- **E-16:** No human access to production data is granted except in documented emergencies such as production stop or similar failures needing for a hot fix.
  - Req_EmergencyAccessRestriction_Org

3.1.3 Metadata

One of the core concepts of IDS is the availability of metadata. This enables data owners to describe their data and therefore make it available for data processors. Data processors can search existing metadata to find the necessary data for their application.

[7] https://industrialdataspace.jiveon.com/docs/DOC-2954
[8] https://industrialdataspace.jiveon.com/docs/DOC-2953

- **E-15:** A set of policies defining critical and non-critical categories in relation to a financial product or categories of financial products.
    - Req_PolicyDefinition

3.2 Organizational Requirements

In the following, more fine-grained requirements with respect to organizational measures are denoted. These serve as a support for compliance with the obligations of data controllers and the rights of data subjects according to the GDPR.

ID	Req_ParticipantCertification
Generic Requirement	With respect to governance in the IDS onboarding process, organizations participating in an IDS ecosystem and process personal data have to be certified (by a trusted third party). A certification ensures that the organization has been verified to have appropriate technical and organizational measures for the protection of personal data in place. In addition to that, the technical component certification, i.e. the certification of IDS connectors and Data Apps running in the connectors, is also desired as stated in Req_ProcessingCertification
Measurement **(How to measure whether the requirement is met?)**	Does the organization possess a commonly accepted data protection certification, such as a TÜV or EuroPriSe seal? Is the organization certified according to the certification process proposed by the IDS RAM? Does the organization possess a valid certificate, e.g. in the form of a digital X.509 certificate, stating that appropriate technical and organizational measures for the protection of personal data are implemented?
Fulfilled by the IDS ecosystem? **(Yes, No)**	Partially, process defined in IDSA Certification Scheme, technical implementation (DAPS etc.) ongoing.
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	No See Art. 42 GDPR, while the IDS certification is not considered to be done by supervisory authorities.

ID	Req_FourEyeLogin_Org
Generic Requirement	The 4-eye/peer principle is applied when analyzing persisted data with human involvement.
Measurement **(How to measure whether the requirement is met?)**	Does the organization possess a commonly accepted data protection certification, such as a TÜV or EuroPriSe seal? Does the organization stick to a documented protocol/policy related to the 4-eye/peer principle? Does the organization perform regular employee trainings with respect to the 4-eye/peer principle?
Fulfilled by the IDS ecosystem? **(Yes, No)**	No* (see explanation at the end of this section)
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	No Not required by GDPR explicitly, but is within the scope of potential organizational measures for integrity and privacy of personal data, e.g. in case of video surveillance. The technical capability of a 4-eye login would support this organizational measure. The implementation cost of such a mechanism appear too acceptable. An example for such sensitive data is video surveillance at workplace and the corresponding processing would by viewing of video stream records by humans.

ID	Req_ContextRelatedSystemDeactivation_Org
Generic Requirement	Depending on a certain context, such as a demonstration, the system that handles personal data is shut down / deactivated by the organization. Otherwise, the personal data may be involuntarily shown to non-authorized persons, e.g. the attendees of a system demonstration.
Measurement **(How to measure whether the requirement is met?)**	Does the organization possess a commonly accepted data protection certification, such as a TÜV or EuroPriSe seal? Does the organization stick to a documented protocol/policy regarding a context-related deactivation of the productive system? Does the organization perform regular employee trainings regarding a context-related deactivation of the productive system?
Fulfilled by the IDS ecosystem? **(Yes, No)**	No* (see explanation at the end of this section)

Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	No Could be derived from Art. 32 (1) lit b. in cases of a a reaction to successful security attacks

ID	Req_EmergencyAccessRestriction_Org
Generic Requirement	Human access to production data is restricted to emergencies only, e.g. a production stop or similar failures needing for a hot fix. Otherwise, humans do not have access to production data at all.
Measurement **(How to measure whether the requirement is met?)**	Does the organization possess a commonly accepted data protection certification, such as a TÜV or EuroPriSe seal? Does the organization stick to a documented protocol/policy regarding the emergency access restriction? Does the organization perform regular employee trainings regarding the emergency access restriction?
Fulfilled by the IDS ecosystem? **(Yes, No)**	No* (see explanation at the end of this section)
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	No Art. 32 GDPR requires confidentiality and integrity of systems and services.

ID	Req_AccessControl
Generic Requirement	Appropriate organizational measures regarding access control are applied. Only relevant personal personnel is granted access to sensitive personal data. The access is granted only by role (RBAC) and data resolution. While Req_DataAccessRestrictions is concerned with the technical implementation of access control, this requirement enables, for instance, the management lists of people who are allowed to access certain data.
Measurement **(How to measure whether the requirement is met?)**	Does the organization possess a commonly accepted data protection certification, such as a TÜV or EuroPriSe seal? Does the organization stick to a documented protocol/policy regarding a role-based access to personal data? Does the organization perform regular employee trainings regarding the role-based data access?
Fulfilled by the IDS ecosystem? **(Yes, No)**	No* (see explanation at the end of this section)
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	Yes Art. 32 GDPR requires confidentiality and integrity of systems and services.

ID	Req_PolicyDefinition
Generic Requirement	Appropriate policies are defined on an organizational level with respect to critical and non-critical categories. For example, this is important for the finance sector. For financial products, a categorization of critical and non-critical finance data is required.
Measurement **(How to measure whether the requirement is met?)**	Does the organization setup appropriate internal policies related to categories of personal data?
Fulfilled by the IDS ecosystem? **(Yes, No)**	No* (see explanation at the end of this section)
Criticality for IDS with respect to GDPR Compliance	Yes This requirement is supported by Art. 47 (2).

(Yes, No)	

ID	Req_ConsentManagement_Org
Generic Requirement	In case, that the lawfulness of the personal data processing is grounded on the consent obtained from the data subject as to Art. 6 (1) lit. a or Art. 9 (2) lit a., organizational measures for the management of the data subjects' consent are required. In particular, this involves the following organizational processes: Storage of consent information, e.g. data subject, date of consent, scope of the consent Possibility for data subjects to withdraw/change the previously provided consent According to the technical equivalent Req_Consent-Management_Tech, a technical implementation for consent management purposes may support and simplify compliance with this GDPR-related aspect.
Measurement **(How to measure whether the requirement is met?)**	Does the organization possess a commonly accepted data protection certification, such as a TÜV or EuroPriSe seal? Did the organization instantiate a protocol to obtain and record the consent of data subjects? Did the organization offer a technical solution allowing data subjects to automatically request information about their previously provided consent as well as to change or even withdraw their consent? Otherwise, did the organization install a data protection officer being available as the contact person for data subjects and offering the stated possibilities for data subjects regarding their provided consent?
Fulfilled by the IDS ecosystem? **(Yes, No)**	No* (see explanation at the end of this section)
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	Yes See Art. 6 (1) lit. a, Art. 7, Art. 8, Art. 9 (2) lit. b GDPR.

ID	Req_DataSubjectRights_TransparentInformation
Generic Requirement	According to Art. 12 - 15 GDPR, the data subject has the right to receive detailed information about the personal data processing. The information especially shall include: purpose of processing categories of personal data recipients the data are shared with duration of data storage source where the data come from (e.g. the data might originate from a third-party source rather than from the data subject himself/herself) existence of automated decision-making, e.g. profiling, and the envisaged consequences of such processing for the data subject
Measurement **(How to measure whether the requirement is met?)**	Does the organization possess a commonly accepted data protection certification, such as a TÜV or EuroPriSe seal? Did the organization instantiate a protocol to provide data subjects with transparent information about the processing of their personal data? Did the organization offer a technical solution allowing data subjects to automatically request information about the data processing? Otherwise, did the organization install a data protection officer being available as the contact person for data subjects and offering the transparent information about the personal data processing on request?
Fulfilled by the IDS ecosystem? **(Yes, No)**	No* (see explanation at the end of this section)
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	Yes See Art. 12 - 15 GDPR.

ID	Req_DataSubjectRights_DataPortability
Generic Requirement	The right to get information about processed personal data (see Req_DataSubjectRights_TransparentInformation) also

	includes the right to get an (electronic) copy/export of such data according to Art. 15 (3) and Art. 20 GDPR.
Measurement **(How to measure whether the requirement is met?)**	Does the organization possess a commonly accepted data protection certification, such as a TÜV or EuroPriSe seal? Did the organization instantiate a protocol to provide data subjects with a copy/export of their personal data and allow it to be transported to another service provider? Did the organization offer a technical solution allowing data subjects to automatically request the copy/export or even the data transfer to another service provider? Otherwise, did the organization install a data protection officer being available as the contact person for data subjects and offering the copy/export/transfer of the personal data on request?
Fulfilled by the IDS ecosystem? **(Yes, No)**	No* (see explanation at the end of this section)
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	Yes See Art. 16 GDPR.

ID	Req_DataSubjectRights_DataCorrection
Generic Requirement	Personal data shall be accurate and kept up-to-date. For this reason, the data subject has the right that the data controller corrects inaccurate personal data and completes incomplete personal data, according to Art. 16 GDPR.
Measurement **(How to measure whether the requirement is met?)**	Does the organization possess a commonly accepted data protection certification, such as a TÜV or EuroPriSe seal? Did the organization instantiate a protocol to enable data subjects to correct inappropriate personal data? Did the organization offer a technical solution allowing data subjects to correct their personal data? Otherwise, did the organization install a data protection officer being available as the contact person for data subjects and offering the correction of the personal data on request?
Fulfilled by the IDS ecosystem? **(Yes, No)**	No* (see explanation at the end of this section)
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	Yes See Art. 16 GDPR.

ID	Req_DataSubjectRights_DataErasure
Generic Requirement	According to Art. 17 GDPR, the data subject has the "right to be forgotten", i.e. the data subject can request the data controller to remove all processed personal data. In case the data have been shared with additional parties, the data controller has to ensure that any links to, copies or replications of the personal data at those parties are deleted as well.

Measurement **(How to measure whether the requirement is met?)**	Does the organization possess a commonly accepted data protection certification, such as a TÜV or EuroPriSe seal? Did the organization instantiate a protocol to enable data subjects to delete their personal data? Did the organization offer a technical solution allowing data subjects to erase their personal data? Otherwise, did the organization install a data protection officer being available as the contact person for data subjects and offering the erasure of the personal data on request?
Fulfilled by the IDS ecosystem? **(Yes, No)**	No* (see explanation at the end of this section)
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	Yes See Art. 17 GDPR.

ID	Req_DataSubjectRights_ProcessingRestriction
Generic Requirement	According to Art. 18 GDPR, the data subject has the right to restrict the processing of his or her personal data.
Measurement **(How to measure whether the requirement is met?)**	Does the organization possess a commonly accepted data protection certification, such as a TÜV or EuroPriSe seal? Did the organization instantiate a protocol to enable data subjects to restrict the processing of their personal data? Did the organization offer a technical solution allowing data subjects to restrict the processing of their personal data? Otherwise, did the organization install a data protection officer being available as the contact person for data subjects and offering the restriction of the personal data processing on request?
Fulfilled by the IDS ecosystem? **(Yes, No)**	No* (see explanation at the end of this section)
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	Yes See Art. 18 GDPR.

ID	Req_DataSubjectRights_ProcessingObjection
Generic Requirement	According to Art. 21 GDPR, the data subject can opt out from the personal data processing at all.
Measurement **(How to measure whether the requirement is met?)**	Does the organization possess a commonly accepted data protection certification, such as a TÜV or EuroPriSe seal? Did the organization instantiate a protocol to enable data subjects to object to the processing of their personal data? Did the organization offer a technical solution allowing data subjects to object to the processing of their personal data? Otherwise, did the organization install a data protection officer being available as the contact person for data subjects and offering the objection of the personal data processing on request?
Fulfilled by the IDS ecosystem? **(Yes, No)**	No* (see explanation at the end of this section)
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	Yes See Art. 21 GDPR.

ID	Req_DataBreachCommunication_SupervisoryAuthority
Generic Requirement	According to Art. 33 GDPR, the data controller has to notify the supervisory authorities in case of a personal data breach. The data controller has to describe the likely consequences of the data breach and document the measures taken or proposed to be taken.
Measurement **(How to measure whether the requirement is met?)**	Does the organization possess a commonly accepted data protection certification, such as a TÜV or EuroPriSe seal? Did the organization instantiate a protocol to notify supervisory authorities in case of a personal data breach? Did the organization install a data protection officer being available as the contact person for supervisory authorities and working together with them in case of a personal data breach?
Fulfilled by the IDS ecosystem? **(Yes, No)**	No* (see explanation at the end of this section)

Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	Yes See Art. 33 GDPR.

ID	Req_DataBreachCommunication_DataSubject
Generic Requirement	According to Art. 34 GDPR, the data controller has to notify the data subject in case of a personal data breach.
Measurement **(How to measure whether the requirement is met?)**	Does the organization possess a commonly accepted data protection certification, such as a TÜV or EuroPriSe seal? Did the organization instantiate a protocol to notify data subjects in case of a personal data breach? Did the organization install a data protection officer being available as the contact person for data subjects and working together with them in case of a personal data breach?
Fulfilled by the IDS ecosystem? **(Yes, No)**	No* (see explanation at the end of this section)
Criticality for IDS with respect to GDPR Compliance **(Yes, No)**	Yes See Art. 34 GDPR.

* This requirement refers to an organizational measure, which is out of scope and responsibility of the IDS ecosystem. Consequently, it cannot be fulfilled by the IDS ecosystem. Instead, the organization participating in the IDS (e.g. a data provider or data consumer as to the definition of the IDS-RAM) is required to internally realize this organizational measure. The column "Measurement" indicates how the requirement may be fulfilled.

4 Categorization and Prioritization of the Technical Requirements

The sections aims at a categorization as well as prioritization of the derived technical requirements with respect to their criticality related to GDPR compliance.

In the following table, we summarize the categories and priorities of the requirements. The priorities are aligned with the facts whether the requirement is already fulfilled by the IDS ecosystem (column "Fulfilled by the IDS ecosystem?" in the requirement tables) and the level of criticality regarding GDPR compliance (column "Criticality for IDS with respect to GDPR Compliance").

Priority	Category Title	Description	Fulfilled by the IDS ecosystem? (Yes, No)	Criticality for IDS with respect to GDPR Compliance (Yes, No)
1a	Must Have	These requirements are mandatory with respect to GDPR compliance and currently not implemented and not planned in the IDS landscape. Thus, the requirements have the highest priority.	No	Yes
1b	Continue Implementing	These requirements are mandatory with respect to GDPR compliance. Currently, they are only partially implemented in the IDS landscape. Consequently, the implementation has to be carried on.	Partially	Yes
2	Keep and Carry On	These requirements are mandatory with respect to GDPR compliance. They have also been successfully been implemented in the IDS landscape. It is important that the features remain and are carried on in future versions of the IDS landscape and IDS RAM, respectively.	Yes	Yes
3	Recommended	These requirements are not critical with respect to GDPR compliance. The GDPR does not require a realization of these	Yes or No	No

		features. Nevertheless, the requirements are recommended and may facilitate the realization of other, mandatory requirements. Implementation of these features would support and simplify GDPR compliance with regard to technical measures.		
4	Uncritical	These requirements are not critical with respect to GDPR compliance. The GDPR does not require a realization of these features. Thus, the requirements are considered as optional.	Yes or No	No

Hereinafter, we associate the technical requirements with the stated priorities/categories.

1a) Must Have

These requirements are mandatory with respect to GDPR compliance and currently not implemented and not planned in the IDS landscape. Thus, the requirements have the highest priority.

Currently, none of the identified requirements are considered as a "must have", meaning that they are critical but not considered in the development, related to GDPR compliance.

1b) Continue Implementing

These requirements are mandatory with respect to GDPR compliance. Currently, there are already efforts being made within the IDS ecosystem to address these concerns, both at the conceptual and implementation level. However, as these efforts have not resulted in fully tested and interoperable implementations at the time of writing, the fulfillment of these requirements with regard to the GDPR can currently not be assessed. Consequently, the current efforts should continue with an additional focus on technical support for GDPR compliance.

- Req_DataAccessRestrictions
    - The usage policy framework currently already includes the capability to restrict access to data based on usage policies. However, care should be given to regularly check alignment of the current state of the usage policy framework implementation with regards to Art. 25 and Art. 32 GDPR. For more details, please see the full description of this requirement in section 2.2.

- Req_UsagePolicyEnforcement
    - In addition, the usage policy framework needs to be able to enforce usage policies. While this is already a priority for the usage policy framework, care should be given to regularly check alignment of the implementation concerning Art. 6 (1), Art. 9 (2), Art. 20 (2) GDPR, as well as in a more general sense Art. 25 and Art. 32 GDPR. For more details, please see the full description of this requirement in section 2.2.

2) Keep and Carry On

These requirements are mandatory with respect to GDPR compliance. They have also been successfully been implemented in the IDS landscape. It is important that the features remain and are carried on in future versions of the IDS landscape and IDS RAM, respectively.

- Req_DataTransferEncryption
    - The IDS RAM already specifies the requirement of encrypted data transfer between connectors. As the GDPR requires protecting personally identifiable data in transit, this feature should never be removed. For more details, please see the full description of this requirement in section 2.2.

3) Recommended

These requirements are not critical with respect to GDPR compliance. The GDPR does not require a realization of these features. Nevertheless, the requirements are recommended and may facilitate the realization of other, mandatory requirements. Implementation of these features would support and simplify GDPR compliance with regard to technical measures.

- Req_DataLabeling
    - In order to simplify GDPR compliant data processing, it is desirable to provide metadata for any data in order to make decision about how to process the data. The initial abstract level of metadata is simple labeling of data, without using any vocabularies or semantics. Examples of such data labeling include a secrecy level, data storage time or access restrictions. For more details, please see the full description of this requirement in section 2.2.
- Req_DomainSpecificVocabularies
    - The next abstraction level in providing metadata towards simplifying GDPR compliant data processing, is to specify domain specific vocabularies. These can e.g. denote the purpose of data processing, the type of data processing or other relevant metadata. For more details, please see the full description of this requirement in section 2.2.
- Req_DataSemantics
    - The final abstraction level in providing metadata towards simplifying GDPR compliant data processing, is to specify the semantics of data which is being processed. For example, it may be required to know about which kind of attributes

in a certain data packet, e.g. a JSON-conformable document, is personal data. Such knowledge about data semantics allows software components, e.g. Data Apps running in the IDS connector, to remove/aggregate/anonymize certain data attributes "on the fly". For more details, please see the full description of this requirement in section 2.2.

- Req_Anonymization
  - According to Recital 26 and Art. 11 GDPR, anonymization is the instrument to leave the GDPR scope. If personal data are anonymized before e.g. transferring them to another IDS participant, the GDPR does not apply for the IDS data consumer receiving the anonymized data. Thus, the anonymization serves as an instrument for data minimization and avoids the processing of personal data at all, where possible. For more details, please see the full description of this requirement in section 2.2.
- Req_Aggregation
  - Analogously to Req_Anonymization, technical capabilities to aggregate attributes from data packets are desirable. Consequently, purpose limitation and data minimization are achieved. For more details, please see the full description of this requirement in section 2.2.
- Req_ConsentManagement_Tech
  - According to the GDPR, the management of data subjects' consent is required, which can serve as legitimation for law-compliant personal data processing. This involves both the storage of consent information, as well as giving data subjects the possibility to withdraw or change previously provided consent. IOSB (Erik Krempel) and IESE (Michael Ochs) have developed confidential examples of systems incorporating consent management that allow for the obtainment and revocation of consent from data subjects, including data categories and data attributes. For more details, please see the full description of this requirement in section 2.2.
- Req_CategoryBasedQueryInterface
  - As soon as metadata in a general sense is available about data offered by data providers, then a query interface is capable to limit data access based on categories in the metadata. This requirement enables a clean separation of concerns between data consumer and data provider. For more details, please see the full description of this requirement in section 2.2.
- Req_UsagePolicyNegotiation
  - While the availability of a usage policy framework for data access restrictions and policy enforcement is a requirement for the technical support of GDPR compliance, the negotiation of usage policies is an optional feature. Policy negotiation could enable more use cases, especially where strict matching is less important. For more details, please see the full description of this requirement in section 2.2.

- Req_AuditLog
  - Providing an implementation of an audit log as an instrument to record processing activities related to personal data in the IDS ecosystem, has the potential to simplify GDPR compliance with regards to technical measures. For instance, this makes it very efficient to support transparency rights towards data subjects (Art. 12 - 15 GDPR). However, it is also possible to address transparency requests by e.g. assigning a system administrator to manually collect the data of a data subject from all potential storage points, and manually prepare a report. Nevertheless, this process is error-prone and accompanied by a huge effort. For more details, please see the full description of this requirement in section 2.2.
- Req_DataStorageEncryption
  - Depending on a risk and data protection impact assessment according to Art. 35 GDPR, it may be required or at least desirable to store personal data in an encrypted manner. In particular, the encrypted storage is advisable for special categories of personal data as to Art. 9 (1) GDPR. In order to facilitate GDPR compliance, the IDS could technically support organizations to increase the level of security regarding the personal data processing (cf. Art. 32 GDPR). The IDS connectors could technically enforce an encrypted delivery to the attached data storage layer, which is used as soon as the IDS-based business use case involves the persistent storage of data in a data sink. Furthermore, the IDS certification process could examine whether the data storage layer attached to the IDS connector operated by the IDS participant uses encryption, e.g. hardware-based full disk encryption. The resulting certificate could transparently state whether the IDS participant stores data in an encrypted way, thus increasing its level of trustworthiness. For more details, please see the full description of this requirement in section 2.2.
- Req_DataSubjectRights_Tech
  - While the data subject rights according to Art. 15 - 22 GDPR are primarily considered as organizational measures, a technical support to facilitate the realization of the data subject's rights is desirable. However, the technical support of these organizational measures can never replace the actual organizational measures. For more details, please see the full description of this requirement in section 2.2.
- Req_DataBreachCommunication_Tech
  - In the case of a personal data breach, the data controller has to inform both the supervisory authority (Art. 33) and the affected data subject (Art. 34). These organizational measures can be supported on a technical level. However, the technical support of these organizational measures can never replace the actual organizational measures. For more details, please see the full description of this requirement in section 2.2.

4) Uncritical

These requirements are not critical with respect to GDPR compliance. The GDPR does not require a realization of these features. Thus, the requirements are considered as optional. However, these requirements each are an important enabler in at least one use case.

- Req_FourEyeLogin_Tech
  - This requirement refers to the capability of enforcing agreement between two humans when viewing data and making decisions based on the viewed data. While this requirement is not part of the GDPR, it can simplify use cases where decisions made by only one person are undesirable. One example, is the reviewing process for video recordings to determine if the footage identifies one or more persons. If the review process is performed by only one person (2 eyes) then the potential for abuse is much higher, than if it is performed two persons (4 eyes). For more details, please see the full description of this requirement in section 2.2.
- Req_ContextRelatedSystemDeactivation_Tech
  - Depending on a certain context, such as a demonstration, the system that handles personal data is shut down / deactivated by the organization. Otherwise, the personal data may be involuntarily shown to non-authorized persons, e.g. the attendees of a system demonstration. This technical measure has to be supported by a corresponding organizational measure, such as listing the persons who are only present for e.g. a demonstration. For more details, please see the full description of this requirement in section 2.2.
- Req_EmergencyAccessRestriction_Tech
  - Human access to production data is restricted to emergencies only, e.g. a production stop or similar failures needing for a hot fix. Otherwise, humans do not have access to production data at all. This technical measure has to be supported by a corresponding organizational measure, such as specifying emergencies. For more details, please see the full description of this requirement in section 2.2.

5 Unique Selling Points

The categorization and prioritization of the technical requirements in the last section rated technical measures according to their criticality for GDPR compliance. On top of that, there is another dimension important for the IDS, namely if a feature would represent a unique selling point (USP). We already see many different technical solutions that allow data processors to work with personal data in a legal way. The goal of the IDS, to achieve a higher level of data control and therefore allow business cases so far not possible with existing technology, would especially benefit if this features would become available. We see multiple such measures that would most likely push the adaption of the IDS for further use cases. Considering this, the following features should be included with a higher priority than is purely motivated by their GDPR compliance rating that is "recommended".

- Req_Anonymization
  - Having a trustworthy and ideally certified processing environment (cp. Req_ParticipantCertification, Req_ProcessingCertification) combined with the possibility to specify measures of anonymization that will be enforced before access would enable many new business applications. These features would be beneficial to all kinds of use cases from advertisement over medical research to financial services.
- Req_Aggregation
  - Similar to Req_Anonymization the specification and "on demand" aggregation of data can help the IDS to reach new markets.
- Req_ConsentManagement_Tech
  - A large part of data processing use cases demand consent of the data subjects. While typically consent management is only done on the highest level, e.g., the data subject consents to all forms of data processing or none, this coarse level of consent management is a typical complain by privacy advocates and increasingly the data protection authorities. Having a finer level of consent management where a data subject can regulate for which application and use cases its data is used, would provide a significant improvement against typical solutions.
- Req_AuditLog
  - Automatically generating an complete audit log is something we so far seldom see in existing software. It would greatly simplify GDPR compliance concerning technical measures. As companies can use these logs to replace error prone and time-consuming alternatives, it would represent an USP.

6 Realization of Organizational Requirements

Apart from the requirements to be implemented on the technical level, GDPR compliance requires the adherence to measures on the organizational level. In the landscape of the IDS, technical measures can be implemented in order to simplify compliance with the GDPR. Nevertheless, GDPR compliance is only fulfilled by the realization of both appropriate technical and appropriate organizational measures.

Independent of the technical specifications in the IDS reference architecture model (IDS-RAM) and software-wise implementations proposed by the IDS initiative, e.g. IDS connectors, the responsibility and accountability with respect to GDPR compliance is on the part of the organization participating in the IDS ecosystem. An organization participating in an IDS-driven use case, in which personal data are processed, has to implement adequate organizational measures for the protection of such personal data.

In general, the organizational measures are outside of the scope of the IDS ecosystem. Consequently, it cannot be said that “the IDS” is GDPR-compliant. Nevertheless, the IDS can support GDPR compliance by extending its certification process with a focus on GDPR-relevant aspects. The IDS certification aims at the assessment of the trustworthiness of organizations and at the adherence to the IDS-RAM specifications. This certification process may be extended by an assessment of GDPR-related aspects on an organizational level. In future work the concrete needs for a GDPR-related certification have to be clarified.

In the following, we will present the organizational requirements regarding the processing of personal data, which are necessary to be implemented in order to comply with the GDPR. As argued above, the responsibility for the realization of these organizational requirements is carried by the organization participating in the IDS.

- Req_AccessControl
  - Organizational policies regulating the access to personal data have to be introduced. For example, it has to be ensured that only relevant personnel is granted access to sensitive personal data. For more details, please see the full description of this requirement in section 3.2.
- Req_PolicyDefinition
  - On the organizational level, appropriate policies with respect to critical and non-critical categories of personal data have to be defined. For example, this is important for the finance sector. For financial products, a categorization of critical and non-critical finance data is required. For more details, please see the full description of this requirement in section 3.2.
- Req_ConsentManagement_Org
  - In case that the lawfulness of the personal data processing is grounded on the consent obtained from the data subject as to Art. 6 (1) lit. a or Art. 9 (2) lit a., organizational measures for the management of the data subjects' consent are required. This includes the recording of the consent information as well as enabling the data subjects to change or withdraw their previously provided

consent. For more details, please see the full description of this requirement in section 3.2.

- Req_DataSubjectRights_TransparentInformation
  - According to Art. 12 - 15 GDPR, the data subject has the right to receive detailed information about the personal data processing. The responsible organization is required to enable the data subjects to exercise their rights. For more details, please see the full description of this requirement in section 3.2.
- Req_DataSubjectRights_DataPortability
  - Furthermore, the right to get information about processed personal data (see above) also includes the right to get an (electronic) copy/export of such data according to Art. 15 (3) and Art. 20 GDPR. The responsible organization is required to enable the data subjects to exercise their rights. For more details, please see the full description of this requirement in section 3.2.
- Req_DataSubjectRights_DataCorrection
  - According to Art. 16 GDPR, the data subject has the right that the data controller corrects inaccurate personal data and completes incomplete personal data. The responsible organization is required to enable the data subjects to exercise their rights. For more details, please see the full description of this requirement in section 3.2.
- Req_DataSubjectRights_DataErasure
  - According to Art. 17 GDPR, the data subject has the "right to be forgotten", i.e. the data subject can request the data controller to remove all processed personal data. The responsible organization is required to enable the data subjects to exercise their rights. For more details, please see the full description of this requirement in section 3.2.
- Req_DataSubjectRights_ProcessingRestriction
  - According to Art. 18 GDPR, the data subject has the right to restrict the processing of his or her personal data. The responsible organization is required to enable the data subjects to exercise their rights. For more details, please see the full description of this requirement in section 3.2.
- Req_DataSubjectRights_ProcessingObjection
  - According to Art. 21 GDPR, the data subject can opt out from the personal data processing at all. The responsible organization is required to enable the data subjects to exercise their rights. For more details, please see the full description of this requirement in section 3.2.
- Req_DataBreachCommunication_SupervisoryAuthority
  - According to Art. 33 GDPR, the data controller has to notify the supervisory authorities in case of a personal data breach. For more details, please see the full description of this requirement in section 3.2.

- Req_DataBreachCommunication_DataSubject
  - According to Art. 34 GDPR, the data controller has to notify the data subject in case of a personal data breach. For more details, please see the full description of this requirement in section 3.2.

7 Summary and Next Steps: Towards Compliance of the IDS with the GDPR

This section outlines the results from the A5 project and summarises our recommendations for the next steps towards enabling GDPR compliance within an IDS based ecosystem both with regards to organisational and technical measures.

The **goal** of the sub-project A5, is to assess the impact of the GDPR (General Data Protection Regulation) on the IDS ecosystem. The GDPR currently is the most important piece of legislation within the EU governing the rules for usage of personally identifiable data in the analogue world as well as in the digital sphere. The GDPR came into effect on 25 May 2018. It defines both the **obligations of the data controllers** and the **rights of the data subjects.** Enabling the respective rights and supporting the respective obligations towards compliance of IT systems with regard to the GDPR always requires **organizational measures** and can in addition be supported by **technical measures**.

While the IDS RAM already specifies approaches for data protection and security, these existing approaches **do not guarantee GDPR compliance** of an implementation of the IDS RAM without additionally taking the requirements of the GDPR into account. In addition, GDPR compliance requires certain organizational measures which fall outside of the conceptual scope of the IDS RAM or of any implementation of the IDS RAM, and which have to be implemented on an organizational level in every single organization, which is deploying any implementation based on the IDS RAM in order to participate in an IDS-based ecosystem.

Therefore, the most important **result** of the A5 sub-project is to list any new requirements, which can be derived from the GDPR, and to make recommendations based on those requirements, which are strictly necessary towards GDPR compliance.

To achieve this classification of requirements, we have taken the following **approach**:

First, we collected use cases from within the IDS and IDS communities, which involve the collection of personally identifiable data.

As a second step, we analyze the use cases to identify their relation to the legal concepts and requirements from the GDPR.

In the third step, we derive so-called epics, from commonly occurring requirements of the use cases or from requirements, which are essential to a single use case. These epics are high-level requirements.

In the fourth step, we break the epics down into more fine-grained requirements, which we set in relation to the conceptual terms of the IDS RAM. We identify both organisational and technical measures as requirements.

Finally, we prioritize the requirements, which we have identified and which are currently not part of the RAM or for which there is no software implementation. The prioritization is based on our understanding of a requirement being strictly necessary for GDPR compliance or not.

In the **document D1 – Identification and Documentation of Relevant Use Cases**[9]**,** we identify and collect **five use cases** from within the IDS and IDS communities, which involve the collection of personally identifiable data. For each use case we describe it from the perspective of the IDS RAM: How does it benefit from the IDS, how would it be implemented using the architectural concepts from the IDS RAM, and how would data processing for the use case be handled by an implementation of the IDS RAM. These use cases are:

Telemedical Lifestyle Intervention Program (TeLiPro) for improved treatment of chronical diseases from the Medical Data Space (MedDS);

Smart Video Surveillance use case from the A3 Civil Security sub-project of the Forschungszentrum Data Spaces (FDS);

Digital Finance Product using Account Information Services (AIS) in Payment Service Directive II (PSD2) based Digital Banking (no data space community);

Account Information Services (AIS) with and without value-added Services in Payment Service Directive II (PSD2) based Digital Banking (no data space community);

Smart Energy Monitoring and Management Services for privately or commercially used residences or offices - from the Energy Data Space.

In the document **D2 – Analysis of the GDPR along the Use Cases**[10]**,** we first summarize the legal concepts from the GDPR. We group them by obligations of the data controllers and the rights of the data subjects. In addition to referencing the respective articles and recitals of the GDPR, we list other interpretative sources. Then we return to the five use cases from D1, and describe them using the legal concepts from the GDPR. In particular, we list for each use case the legal roles of all actors. Then we list how personal data is processed in the use case, by enumerating each data type, which actor is processing it, how it is processed and for which purpose. Then we derive commonalities and differences in how the use cases relate to the GDPR in three areas: (1) the flow of data and processing, (2) a privacy-related risk analysis, (3) generalizability to other applications and domains. Based on this we formulate epics, which apply to the data origin/collection point, to the data transfer or to data destination/processing. We also include a traceability matrix, which connects the epics to the use cases.

In **this paper,** we decompose the epics into more fine-grained requirements, which we set in relation to the conceptual terms of the IDS RAM. We identify both organizational and technical measures as requirements, and we sort them by the following categories: (1) processing, (2) storage, (3) access control, usage control & security, (4) metadata. Then we describe for each requirement how we measure/check whether the requirement is met, and we list if the requirement is fulfilled by the IDS RAM or other specifications of the IDS. We also list if the requirement is critical for GDPR compliance and reference the supporting GDPR articles.

[9] https://industrialdataspace.jiveon.com/docs/DOC-2954
[10] https://industrialdataspace.jiveon.com/docs/DOC-2953

Moreover, we categorize and prioritize the technical requirements as follows:

1) a. "must have" requirements, which are technical measures, strictly required for GDPR compliance, which are currently not included in the IDS RAM or any other specification of the IDS. **Our assessment:** There are **no** such requirements.

1) b. "continue implementing" requirements, which are technical measures, strictly required for GDPR compliance, and which are present in the IDS RAM, but where current implementations are unfinished, so that GDPR compliance cannot be assessed. **Our assessment:** There are **two** such requirements, which are both part of the usage policy framework in the IDS landscape. As we estimate that the implementation complexity of these features is high, we recommend accelerating current efforts towards fully tested and interoperable implementations and alignment with the listed parts of the GDPR.

2) "keep and carry on" requirements which are mandatory technical measures with respect to GDPR compliance, and which have been successfully been implemented in the IDS landscape. They should never be removed. **Our assessment:** this is **one** requirement, and it should be feasible to maintain it.

3) "recommended" requirements are not critical with respect to GDPR compliance. Implementation of these requirements would support and simplify GDPR compliance with regard to technical measures and may facilitate the realization of other, mandatory requirements. In several cases, a technical measure can support and simplify a mandatory organizational measure. In such cases, while the organizational measure is mandatory, the technical measure is not mandatory. **Our assessment:** there are **twelve** such requirements. We would recommend prioritizing them based on industry feedback. Our first priority would be implementing requirements, which provide technical support to automate critical aspects of the GDPR, which otherwise can be performed as organizational measures, but with a high loss of efficiency and therefore much higher costs (Req_AuditLog, Req_ConsentManagement, Req_DataSubjectRights_Tech, Req_DataBreachCommunication_Tech). Our second priority would be to implement requirements, which can unlock the value in personal data by removing personal identification details in a sustainable way. This enables unlimited processing beyond consent management or usage control (Req_Anonymization, Req_Aggregation). While the recommended features are not critical with respect to GDPR compliance, many of them may serve as a unique selling point (USP) of the IDS enabling the adoption of new business-relevant use cases and pushing the dissemination of the IDS in general. For a more detailed description of the USPs, please see section 5.

4) "uncritical" requirements, which are not critical with respect to GDPR compliance. However, these requirements each are an important enabler in at least one use case. **Our assessment:** there are **three** such requirements. We recommend implementing them when they are actually needed by an industry partner.

Furthermore, we have identified four requirements, which could represent **unique selling points (USP)** of the IDS towards the goal of achieving a higher level of data control and therefore allow business cases so far not possible with existing technology. These USP enabling requirements are the implementation of anonymization and aggregation approaches, technical support of consent management, as well as an implementation of an audit log.

In addition to a categorization of technical measures towards GDPR compliance, we also have identified **organizational measures** towards GDPR compliance. These organizational measures are always mandatory at an organizational level in every single organization, which is deploying any implementation based on the IDS RAM in order to participate in an IDS-based ecosystem.

Our assessment: there are **eleven** such organizational measures. We recommend including them as part of the IDS certification process. This could allow certifying GDPR compliance of an organization as part of IDS certification. However, establishing the legal requirements for including GDPR compliance in the IDS certification process would require legal advice from lawyers specialized in the GDPR.

Summarizing the most important take-away messages, please also take note of the Executive Summary at the beginning of this paper.

OUR MEMBERS

- Aalto University
- ADVANEO
- agmadata DIGITALE PROZESSE FÜR GUTE LEBENSMITTEL
- Allianz
- AtoS
- Audi
- bill-X Collect. Manage. Execute.
- Boehringer Ingelheim
- Brainport Industries
- bdr. BUNDESDRUCKEREI
- CAICT 中国信息通信研究院
- CANADA'S DIGITAL TECHNOLOGY SUPERCLUSTER
- CDQ SHARING DATA EXCELLENCE
- cea
- Cefriel POLITECNICO DI MILANO
- iti Information Technologies Institute
- CHALMERS UNIVERSITY OF TECHNOLOGY
- COSMOPlat
- Cybus
- CTU CZECH TECHNICAL UNIVERSITY IN PRAGUE
- DAIMLER
- DATAAHEAD
- DATATRONiQ
- DB SCHENKER
- Deloitte.
- Deutsche Bank
- DGZfP
- DHBW Duale Hochschule Baden-Württemberg Ravensburg
- DigitalGreen
- DIMECC
- DR. SCHNEIDER UNTERNEHMENSGRUPPE
- eccenca command your data!
- EcoDataCenter
- ELDORADO
- engie
- ENGINEERING
- 8760 Fastems
- fir an der RWTH Aachen
- FIWARE
- Leibniz Universität Hannover
- Fraunhofer
- GateHouse Logistics
- GERMAN EDGE CLOUD
- GESIS GESELLSCHAFT FÜR INFORMATIONSSYSTEME
- Google
- HITACHI Inspire the Next
- HUAWEI
- i2cat
- automotive engineering iav
- IBM
- ILVO Instituut voor Landbouw-, Visserij- en Voedingsonderzoek
- imec
- Imperial College London
- Institut Mines-Télécom
- INDUSTRY 2025 INDUSTRIE INDUSTRIA
- INNOPAY
- innovalia ASSOCIATION
- Insight
- Irish Manufacturing Research
- ITI INVESTIGATE TO INNOVATE
- Klarrio
- K
- KOMSA DIE BESSERE VERBINDUNG
- LOSEC LEADERS IN SECURITY
- Lobster
- Logata Digital Solutions
- LOGENIOS
- minnosphere
- .msg
- nexedi
- nicos AG
- olmogo data ownership solutions

orbiter

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

pi-lar GmbH

POLITECNICO MILANO 1863

pwc

QuinScape

realworldsystems

RI.SE

REWE GROUP

RITTAL

SALZGITTERAG Stahl und Technologie

SAP

SCHAEFFLER

SETLOG The Smart Connective

SICK Sensor Intelligence.

SIEMENS Ingenuity for life

Signal Solutions

SINTEF

SMEV AG Smart Mobility Evolution

TARC Tunku Abdul Rahman University College

tecnalia Inspiring Business

IK4 TEKNIKER Research Alliance

T

mtc Manufacturing Technology Centre

thyssenkrupp

TNO innovation for life

TÜV NORD GROUP

TÜV SÜD

UNIKLINIK RWTH AACHEN

UNiSCON Sealed Cloud Technologies

UNITY CONSULTING & INNOVATION

universität Witten/Herdecke

University of Amsterdam

UNIVERSITY OF TWENTE.

vastuu group

VDMA

VOLKSWAGEN AKTIENGESELLSCHAFT

VTT

welotec a byte smarter

WeTech IDS-China

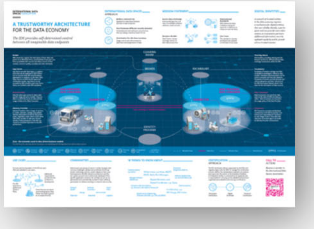
ZVEI: Die Elektroindustrie

OVERVIEW PUBLICATIONS

Reference Architecture Model

Executive Summary

Image Brochure



Infographic

Use Case Brochures

Study on Data Exchange

Position Paper Implementing the European Data Strategy

Position Paper GDPR Requirements and Recommendations

Position Paper Usage Control in the IDS

Position Paper IDS Certification Explained

White Paper Certification

Sharing data while keeping data ownership

Magazine Data Spaces_Now!

For these and further downloads: www.internationaldataspaces.org/info-package

Code available at: https://github.com/industrial-data-space

CONTACT

Head Office

INTERNATIONAL DATA SPACES ASSOCIATION

Emil-Figge-Str. 80
44227 Dortmund | Germany

phone: +49 231 70096 501
mail: info@internationaldataspaces.org

WWW.INTERNATIONALDATASPACES.ORG

@ids_association

international-data-spaces-association