Data Management SPICE PAM 2.0; Applications in the context of the EU AI Act and EU DATA Act

Dr. Reiner Seitz

APS Advanced Project Services SRL

reiner.seitz@aps-srl.ro

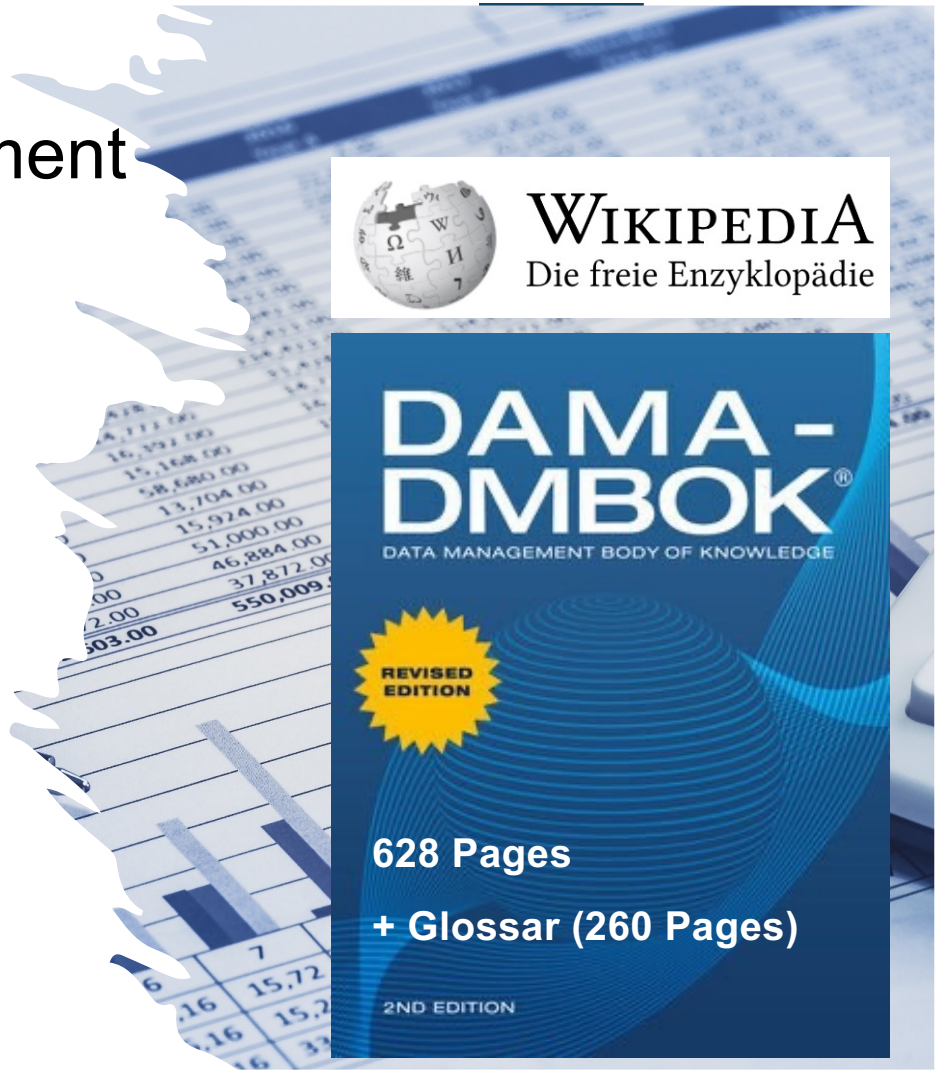
Trying a definition of Data Management

Data Management is the

- set of all methodological, conceptual, organizational, technical measures and procedures
- for handling the resource "data“,
- with the aim of introducing them into business processes
- with their maximum potential for use. (1)

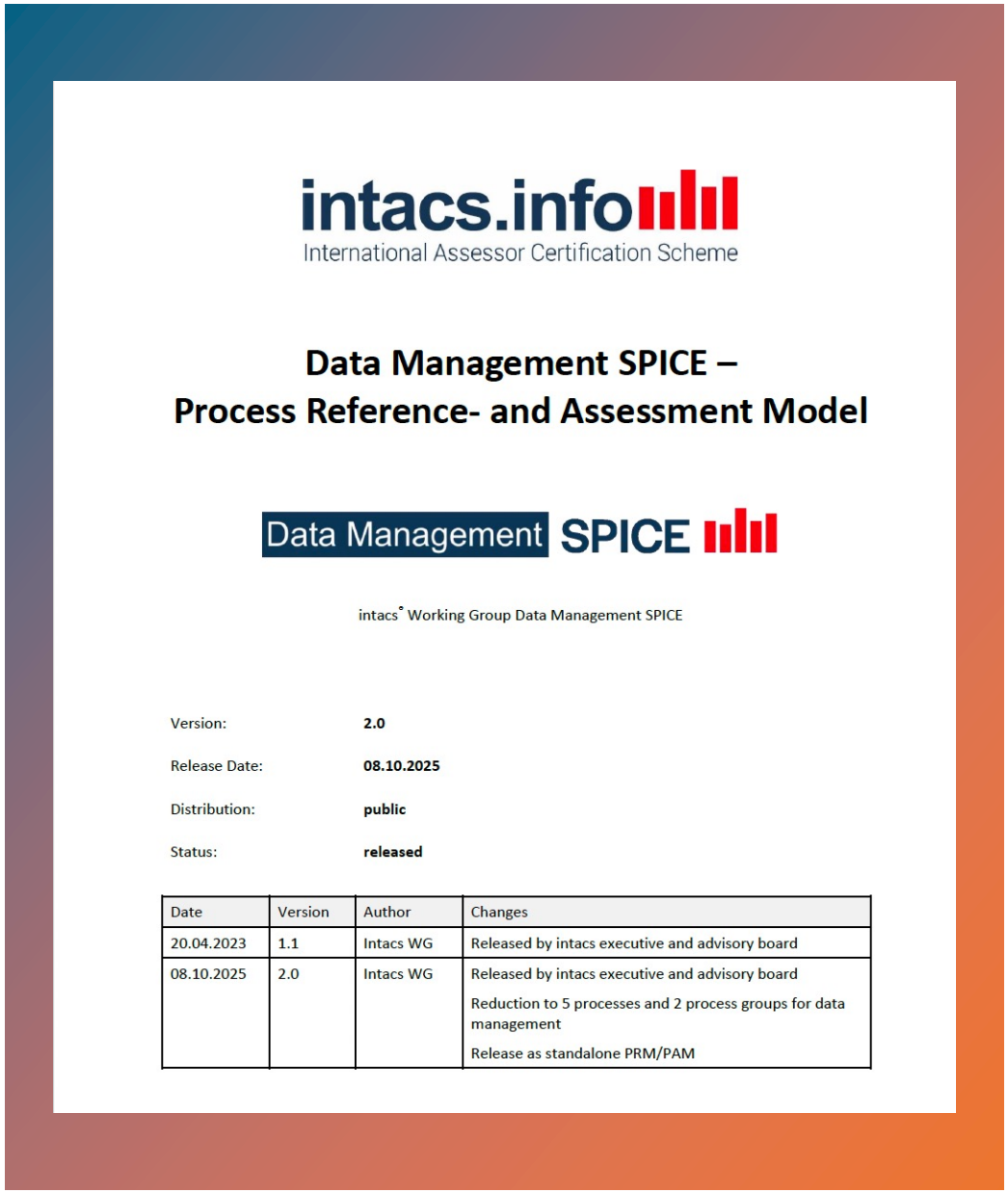
Data Management is

- the development, execution, and supervision
- of plans, policies, programs, and practices
- that deliver, control, protect, and enhance the value of data and information assets
- throughout their lifecycles. (2)



1 Based on Wikipedia: https://de.wikipedia.org/wiki/Datenmanagement
2 DAMA DMBOK 2.0 Revision 2024 (Data Management Body of Knowledge)

INTACS®



intacs.info
International Assessor Certification Scheme

Data Management SPICE –
Process Reference- and Assessment Model

Data Management SPICE

intacs® Working Group Data Management SPICE

Version: **2.0**

Release Date: **08.10.2025**

Distribution: **public**

Status: **released**

Date	Version	Author	Changes
20.04.2023	1.1	Intacs WG	Released by intacs executive and advisory board
08.10.2025	2.0	Intacs WG	Released by intacs executive and advisory board Reduction to 5 processes and 2 process groups for data management Release as standalone PRM/PAM

APS. Advanced Project Services
STRENGTHEN PROCESSES. ADVANCE PERFORMANCE.

Data Management v2.0

Download:

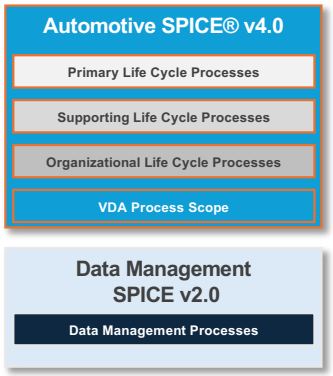
https://intacs.info/component/rsfiles/download-file/files?path=SPICE%2BDocuments%252FDataManagement%252FData%2BManagement%2BSPICE%2BPAM%2BV2.0.pdf&Itemid=104

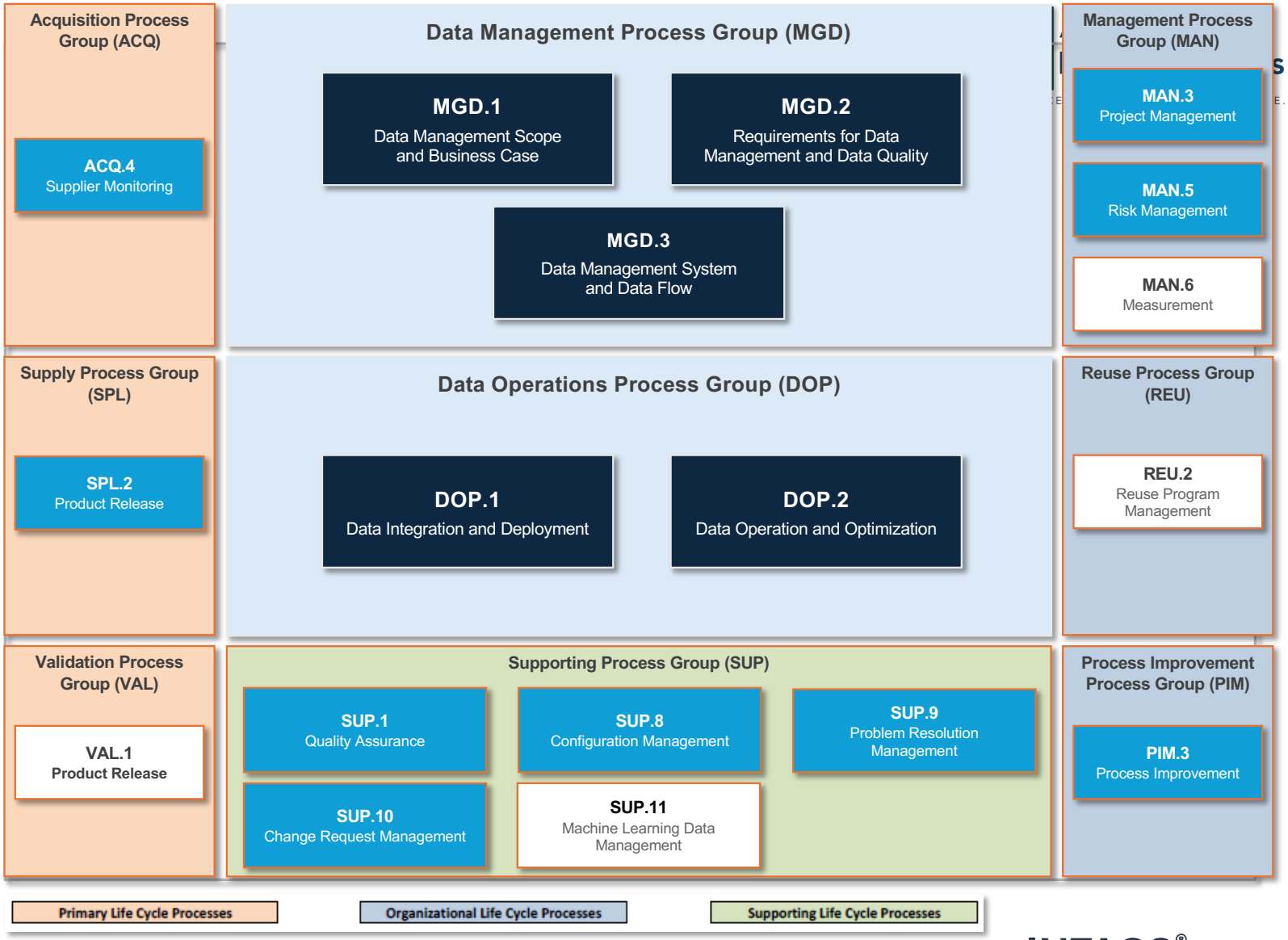
Data Management SPICE v2.0

in context of
Automotive SPICE® 4.0
usable as Plug-In or
Standalone PRM/PAM

SUP.11 of ML SPICE
overlaps with the DM SPICE processes but is significantly shorter and less detailed than in DM SPICE.

In case DM SPICE is applied SUP.11 can be descoped.





DM SPICE Processes (1/2)

We broke down several parts of a Data Management SPICE-style lifecycle into clear intent and dependencies:

MGD.1 sets the foundation: define scope/governance/data types, manage stakeholders, align a business case, and maintain a shared business glossary so everyone agrees on purpose and terminology.

MGD.2 turns needs into a controlled requirements system: use operational scenarios to elicit needs, agree stakeholder requirements, derive functional/non-functional requirements, validate them, ensure traceability, and communicate them aligned to scope and purpose.

MGD.3 translates requirements into solution design: maintain a technical concept, define data flows, choose data sources, mark authoritative sources, set demarcation points, define data quality rules, build a conceptual schema, and enforce consistency/traceability between requirements, concept, and flows.

DM SPICE Processes (2/2)

DOP.1 prepares and executes integration/deployment: define the integration & deployment approach, apply data quality checks during integration and deployment, prepare stakeholders, then deploy and resolve issues.

DOP.2 runs and improves operations: define an operations & optimization approach, continuously monitor system performance, data quality, and governance compliance, and ensure operations keep serving the intended purpose—with recording/evaluation/communication as a recurring feedback loop.

Overall, the dependency chain we established is:

Purpose & alignment (**MGD.1**) → Requirements (**MGD.2**) → Architecture & data design (**MGD.3**) → Integration & deployment (**DOP.1**) → Operations & continuous improvement (**DOP.2**), with traceability and communication acting as cross-cutting controls to keep everything consistent and goal-driven.

Digital Regulation in the last Decade

EU regulation set		US regulations
GDPR Personal data regime; entered into force 2016, applies from 25 May 2018.	2016	**21st Century Cures Act** Health-data interoperability; information-blocking compliance from Apr 2021.
Market access + cyber foundations Geo-blocking; Single Digital Gateway; Free Flow of Non-Personal Data; Cybersecurity Act; P2B.	2018–20	**Cross-border data + IoT + CCPA** CLOUD Act; IoT Cybersecurity Improvement Act; California CCPA effective Jan 2020.
Platforms, data sharing, resilience Terrorist Content Online; Data Governance Act; DMA; DSA; DORA.	2021–22	**Cybersecurity federal regulations** EO 14028; FTC Safeguards; CIRCIA; OMB M-22-18 software attestations.
Data Act Data Act adopted 2023 and entered into force Jan 2024.	2023	**Cyber disclosure + AI EO + state privacy** SEC cyber disclosure; EO 14110 on AI; VA/CO/CT/UT privacy wave.
AI, identity, infrastructure, cyber products Interoperable Europe; eIDAS 2.0; Gigabit Infrastructure; AI Act; Cyber Resilience Act.	2024	**AI and privacy** FCC Open Internet order stayed/set aside; Utah AI Act; Colorado AI Act; FL/TX/OR/MT privacy laws.
Application wave Data Act Sep 2025; AI Act phased 2025–26; CRA 2026/27; EHDS from 2027.	2025–27	**State regulation wave** 2025 AI executive order; IA/DE/NE/NH/NJ/TN/MN/MD privacy; 2026 CO AI Act + IN/KY/RI privacy.

EU = harmonized, directly applicable regulation set; US = fragmented but evolving mix of federal rules, agency rules and state privacy/AI laws.

EU AI Act

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations and Directives — Artificial Intelligence Act. Published in the Official Journal of the European Union, OJ L, 2024/1689, 12 July 2024.

- Reference: https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Timeline

1. August 2024	The AI Act entered into force.
2. February 2025	Chapters I and II apply, including general provisions and prohibited AI practices.
2. August 2025	Rules on general-purpose AI, governance, penalties, confidentiality, and related provisions apply, with some exceptions.
2. August 2026	Most of the AI Act applies.
2. August 2027	Article 6(1) and corresponding obligations for certain high-risk AI systems apply.

The legal basis is Article 113 of Regulation (EU) 2024/1689, setting the staggered application timeline

Purpose & Scope of EU AI Act

- Create one EU-wide legal framework for AI
- Promote human-centric and trustworthy AI
- Protect health, safety, and fundamental rights
- Risk-based approach to categorize AI
- Prohibited AI practices
- High-risk AI systems
- Transparency and general-purpose AI

Data and data governance see: https://artificialintelligenceact.eu/article/10/

EU AI Act & DM SPICE

Governance & Scope

AI Act sets the need for intended purpose, risk classification, role clarity, and governance of training, validation, testing, input and operational data.

DM SPICE MGD.1 requires the definition of scope, governance constraints, data types, stakeholder map, business case, security goals, and glossary.

Requirements & Architecture

AI Act obligations include data-quality, provenance, representativeness, bias, traceability, logging and documentation requirements.

DM SPICE MGD.2 and MGD.3 require traceability, technical concepts, data flows, authoritative sources, demarcation points, and quality rules.

Deployment & Operations

AI Act compliance must continue from dataset release into live AI use, monitoring, change control, and post-market evidence.

DM SPICE DOP.1 and DOP.2 require deployment readiness, integration, operational monitoring, governance, optimization, and data-quality control.

Quality, Evidence & Assurance

AI Act needs reliable, representative, bias-controlled and defensible data plus demonstrable conformity evidence.

DM SPICE requires quality criteria, rules and thresholds, governance controls, traceability, problem/change management, and assessment evidence.

The EU AI Act defines what must be controlled for trustworthy AI;
DM SPICE provides the evaluation framework for the maturity of the implementation, monitoring and evidence in practice.

EU Data Act

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). Official Journal: OJ L, 2023/2854, 22 December 2023.

- http://data.europa.eu/eli/reg/2023/2854/oj

Timeline

11. January 2024	The Data Act entered into force.
12. September 2025	Most provisions became applicable.
12. September 2026	The obligation in Article 3(1) applies to connected products and related services placed on the market after this date.

Purpose & Scope of EU Data Act

- Remove barriers to data sharing in the EU single market.
- Create harmonised rules on who can use data and under what conditions.
- Give users of connected products and related services access to their data.
- Ensure fair business-to-business data access.
- Enable public-sector access in exceptional situations.
- Support cloud provider switching and interoperability

Purpose & Scope of EU Data Act

Article 10: Data and Data Governance

Date of entry into force: **2 August 2026**

According to: **Article 113**

See here for a full implementation timeline.

SUMMARY +

1. High-risk AI systems which make use of techniques involving the training of AI models with data shall be developed on the basis of training, validation and testing data sets that meet the quality criteria referred to in paragraphs 2 to 5 whenever such data sets are used.

2. Training, validation and testing data sets shall be subject to data governance and management practices appropriate for the intended purpose of the high-risk AI system. Those practices shall concern in particular:

(a) the relevant design choices;

(b) data collection processes and the origin of data, and in the case of personal data, the original purpose of the data collection;

(c) relevant data-preparation processing operations, such as annotation, labelling, cleaning, updating, enrichment and aggregation;

Source: https://artificialintelligenceact.eu/article/10/

EU Data Act & DM SPICE

Governance & Scope

EU Data Act sets the need for clear access, transparency, safeguards, and accountability.

DM SPICE MGD.1 requires the definition of scope, governance constraints, stakeholder map, business case, and glossary.

Requirements & Architecture

Data Act obligations must be translated into structured access, sharing, protection, and portability requirements.

DM SPICE MGD.2 and MGD.3 require traceability, technical concepts, data flows, authoritative sources, and demarcation points.

Deployment & Operations

Compliance must work in live operations, not only in policy or contracting.

DM SPICE DOP.1 and DOP.2 require deployment readiness, integration, monitoring, governance, and data-quality control.

Quality, Evidence & Value

The Data Act needs reliable, usable, and defensible data plus demonstrable compliance.

DM SPICE requires data-quality rules, governance controls, and assessment evidence for sustained management oversight.

The EU Data Act defines what must be enabled and protected;
DM SPICE provides the evaluation framework for the maturity of the implementation, monitoring, and evidence in practice.

Summary

- **Data management** is the coordinated set of methods, policies, processes, organizational measures, and technical controls used to manage data as a business asset throughout its lifecycle.

- **Data Management SPICE v2.0** can be used either as a plug-in to **Automotive SPICE 4.0** or as a standalone process reference and assessment model (PAM).

- **Data Management SPICE can** support the evaluation of compliance of data managemt for the increasing number of digital regulations

  Examples **EU AI Act** and **EU Data Act**.

- **Takeaway:**

  DM is a structured operational bridge between regulatory obligations and practical data governance. It can help organizations turn EU AI Act and EU Data Act requirements into defined scope, traceable requirements, technical architecture, deployment controls, operational monitoring and data quality evidence. Then DM SPICE supports organisations to assess and understand their process maturity.