Statement

Review of the **European Interoperability Framework (EIF)**

As an international group of companies, msg supports clients from various sectors throughout the entire digitalisation process – from strategy and transformation consultancy, through the implementation of suitable solutions, to operations and service. In the public sector, we have many years' experience in national and international digitalisation projects. We therefore explain recommendations regarding the call for evidence on the European Interoperability Framework (EIF) using selected examples from our project work.

Interoperability should be understood more strongly within the EIF as a practical implementation task – not merely as a collection of technical standards.

This requires concrete *reference architectures, machine-readable data models, clear responsibilities, API/event contracts, test criteria and procurement requirements* that can be directly applied in public sector projects.

Our practical experience in IT consultancy and implementation projects shows that interoperability often fails due to a lack of harmonisation – for example, in data mapping, register links, data protection roles, federal or Europe-wide subsidiary competences, legacy system integrations and AI-compatible data quality.

As the EIF is not binding and interoperability initially entails additional coordination efforts, decision-makers must be given greater incentives to adopt it through demonstrable benefits, concrete incentives and national contact points.

The EIF should therefore be further developed into a manageable framework that supports the development of interoperable business processes in the Member States. As a key measure, we propose the development of domain-specific reference architectures and reference solutions.

Question 1 – Retain or expand

"What elements of the previous EIF versions should be kept or strengthened?"

In particular, the EIF's four-level model should be retained; its translation into concrete, reusable project artefacts must be expanded. The model is useful in practice because it prevents interoperability from being treated prematurely as purely an interface issue. Federal data exchange can only function effectively if the legal basis, purpose limitation, responsibilities, data significance, operational responsibility and technical implementation are consistently aligned.

At the legal level, the EIF should in future provide templates for cross-agency data sharing, such as a Data Sharing & Accountability Sheet. In security-related areas such as data exchange between immigration authorities or police agencies, the legal basis, purpose limitation, roles, protection requirements, logging, retention periods and accountability should be documented in an auditable format. This would ensure that data protection is not treated retrospectively as an obstacle, but rather as an integral part of the interoperability design from the outset.

At the organisational level, the EIF should describe the governance of integrated public services more precisely by defining organisational responsibility for data products, registers, interface quality, versioning, operation and technical approval. Roles such as Data Steward, Register Manager, API Product Owner, Technical Product Manager and Interface Manager should therefore be described as reusable role profiles.

At the semantic level, SEMIC Core Vocabularies and comparable European building blocks should be retained, but made compatible with national standards such as XÖV and FIM in Germany, for example. Specific areas of application include statistical and register data at the Federal Statistical Office and the Federal Office of Administration, or vehicle and mobility data at the Federal Motor Transport Authority and the Federal Ministry of Transport, as well as structured application and supporting documentation data in funding procedures.

At a technical level, the EIF should retain proven European building blocks, such as those for electronic identities, secure delivery, the 'once-only' principle and reusable digital components. At the same time, these building blocks should in future not only be described but also supplemented by concrete reference solutions.

Above all, project teams need practical templates for interfaces, event notifications, authentication, role and rights concepts, logging, test data, system deployment and subsequent replacement. Such templates would help public authorities to avoid having to redesign interoperable solutions from scratch for every project, but instead to draw on tested and reusable approaches.

Examples such as the Federal Motor Transport Authority's interfaces for major clients, the Federal Office for Economic Affairs and Export Control's online portals, the Federal Environment Agency's data platforms, the Federal Office for Information Security's minimum cloud standards, and the Federal IT Centre's platform services demonstrate that the greatest practical benefit arises where the EIF provides concrete technical guidance for real-world administrative projects.

Conclusions for the EIF:

This response highlights, in particular, the need for further specification in the EIF's recommendations on reuse, open standards, data portability, and security and data protection. In future, these should be underpinned more robustly by verifiable minimum deliverables, such as role definitions, data models, interface specifications, quality rules, test data, and operational and migration plans.

Question 2 – Major barriers to implementation

"What are the main barriers for implementing the EIF at EU, national, regional or local level?"

The greatest obstacles to the implementation of the EIF do not lie in a lack of commitment to interoperability, but in the institutional costs, risks and uncertainties involved in achieving it in practice. Interoperability initially entails more effort: public authorities must coordinate across jurisdictional boundaries, harmonise terminology and data models, clarify legal and data protection issues, integrate legacy systems and synchronise their own project priorities with external dependencies. As the EIF is not binding, a clearer logic of benefits and incentives is required.

One particularly prominent obstacle is the exchange of information at federal level in security-related domains. In the collaboration between the Federal Criminal Police Office, the State Criminal Police Offices and the state police forces, situation picture and data on individuals, cases, objects and incidents are required, each of which is characterised by different legal, organisational and technical aspects. The hurdle rarely lies solely in the interface, but rather in differing security requirements, responsibilities, data models, authorisation processes, operational models and levels of maturity.

The EIF should incorporate such domains as model cases for a federal data and event model and, in particular, provide structured guidelines for integration with Europe-wide systems.

Similar hurdles arise in migration and register chains, for example between the Federal Office for Migration and Refugees, the Federal Police, immigration authorities and related processes. In these contexts, identities, status events, supporting documents, decisions and follow-up processes must be transferred consistently.

Obstacles arise from media breaks, inconsistent status and evidence models, issues of purpose limitation, legacy system integration and unclear responsibilities for data quality. An EIF that describes such register events as reusable templates would significantly facilitate the transition from guidelines to implementation.

Interoperability fails in this context due to issues with *semantics, metadata, quality rules, API capability* and differing *operational responsibilities.*

Added to this is a governance and procurement dimension: EU timetables, specifications and interfaces often evolve over extended periods; national authorities, however, must plan, secure funding and carry out development at an early stage. Repeated delays or changes undermine confidence in planning and result in scarce resources being diverted to projects with more immediate deadlines. At the same time, procurement creates new siloed solutions if OpenAPI/AsyncAPI, data export, test data, versioning, auditability, exit capability and data portability are not specified as *verifiable quality criteria.*

Conclusions for the EIF:

The implementation barriers outlined above highlight a particular need for revision in the EIF areas of governance, organisational coordination, semantic harmonisation and technical interoperability. In these areas, typical implementation hurdles should be addressed more specifically, such as inconsistent status models, unclear data ownership, federal responsibilities, legacy systems, changing European specifications and a lack of interface patterns.

Question 3 – Additional guidance

"What additional guidance would facilitate a more systematic uptake?"

The future EIF should not merely set out principles, but should provide public authorities with a practical toolkit for implementation. What is needed are concrete guidelines, templates and assessment criteria that enable interoperability to be implemented directly in specialist procedures, tenders, architectural decisions and projects. Only in this way will a voluntary European framework become an effective tool for digital public administration.

Additional guidelines should further develop the European Interoperability Framework, moving it away from being merely a strategic guide towards becoming a practical implementation framework. It is not enough to describe principles such as reusability, openness or user-centredness in abstract terms.

Public authorities and project teams need concrete tools that they can apply directly in business processes, tenders, architectural and implementation projects.

A European interoperability implementation toolkit would be useful. This should consist of practical templates, for example for reference architectures, data models, interface descriptions, event messages, role and rights concepts, data protection and security requirements, test data, quality rules and procurement clauses. This would not make the framework more binding in a legal sense, but it would be significantly more effective in practical application. Public authorities would not have to reinterpret interoperability anew in every project, but could instead draw on tested and reusable patterns.

Domain-specific guidelines for typical administrative workflows would be particularly helpful. These include, for example, federal information exchange in the police sector, migration and register processes, access to health data, the modernisation of statistics and registers, environmental and geodata, mobility and infrastructure data, as well as funding and verification procedures. In such areas in particular, interoperability problems do not arise at a single interface, but rather from the interplay of legal frameworks, responsibilities, data meanings, data protection, legacy systems and organisational accountability.

A guide to police information exchange could, for example, describe how case, personal, property and incident data can be exchanged at federal level, which data protection requirements must be taken into account, how access is logged, and how data remains usable for situational assessments or analytical evaluations. A guide for migration and register chains could include templates for status data, supporting documents, identity checks, handover procedures and incident reports. For health, environmental or statistical data, metadata, data quality, pseudonymisation, controlled data access and interoperability with European data spaces would be particularly crucial.

In addition to such technical guidelines, the future EIF should include a maturity model. This should enable public authorities to assess their own level of interoperability: Have the legal bases been clarified? Are there common data models? Have responsibilities been defined? Are interfaces documented and testable? Can data be used securely, transparently and in a way that allows for reuse? Such a model would make interoperability more measurable and help to identify risks at an early stage in projects, architectural decisions and procurement processes.

A procurement guide is also of particular importance. Many new siloed solutions arise not from a lack of willingness to achieve interoperability, but because tenders do not specify requirements for them in sufficient detail. The EIF should therefore provide model wording and assessment criteria, for example for open interfaces, data export, versioning, testability, logging, role and rights concepts, system replaceability and data portability. Interoperability would thus not only become apparent retrospectively as an integration problem, but would be taken into account as a quality criterion right from the tendering stage.

Finally, guidelines should also highlight the benefits of interoperability more clearly. As the EIF is not binding and interoperability initially involves additional coordination efforts, public authorities must be able to recognise the specific added value they will gain: lower integration costs, better data quality, fewer data discontinuities, faster implementation of European requirements, better reuse of existing solutions and greater interoperability with future digital services. Only when these benefits become apparent can a voluntary framework become a truly effective tool for the digital transformation of public administration.

Implications for the EIF:

This response highlights a particular need for further development in the EIF areas of organisational, semantic and technical interoperability, as well as in the model for integrated public services. These areas should be operationalised through specific guidelines for typical administrative workflows, such as those relating to police information exchange, register processes, health data, environmental and geodata, mobility data, and funding and verification procedures.

Question 4 – Supporting digital transformation

"How can the future EIF support the next steps in the digital transformation of public administrations?"

The future EIF should define interoperability as the foundation for the next stage of digitalisation in public administration: 'once-only' principles, European data spaces, data-driven services, AI support and digital sovereignty cannot be sustainably achieved without robust legal, organisational, semantic and technical interoperability. The EIF should not treat these issues as an additional chapter, but as a further development of its core mandate.

There is a two-fold relationship with AI. On the one hand, interoperability is a prerequisite for responsible AI in public administration: models and assistance systems require clear data provenance, machine-readable semantics, metadata, quality indicators, rights and role models, audit logs, test data and human approval.

On the other hand, AI itself can support interoperability, for example through schema mapping, the detection of semantic duplicates, data quality checks, test case generation, migration analysis, interface documentation and conformity checks. AI can bridge heterogeneity, but it does not replace professional responsibility for the meaning, quality and use of public administration data.

The EIF should therefore include a chapter on 'AI-ready interoperability'. For statistics and register modernisation, this would mean standardising identifiers, metadata, data quality metrics and change events in such a way as to enable 'once-only' data collection, the reduction of red tape and AI-supported analyses. For police situational picture, this would mean modelling data objects, protection requirements, origin, authorisations and search/analysis logs in a traceable manner. For health data repositories, this would mean recognising pseudonymisation, secure analysis environments and metadata catalogues as interoperability requirements.

The environmental, mobility and funding sectors also demonstrate how digital transformation can benefit from the EIF. Environmental and geodata require standardised temporal and spatial references, quality indicators and data publication patterns; mobility and infrastructure data require reliable interfaces between registers, operators and real-time data; funding procedures require structured applications, supporting evidence, register reconciliations and status events rather than document-heavy verification processes. In all cases, digitalisation will only become scalable once data is treated as reusable, quality-assured administrative resources.

The EIF should consistently operationalise digital sovereignty as a matter of interoperability. Sovereignty arises not solely through European operations, but through open standards, portable data, interchangeable components, traceable interfaces, open-source options, exit scenarios, cryptography and identity requirements, and connectivity to European cloud and data space structures. National platform approaches (such as those at ITZBund, the Federal Office for Information Security, the Federal Ministry for Digital Affairs and State Modernisation, PLAIN/KIPITZ or services affiliated with the Federal Printing Office) can serve as points of integration for this purpose, provided they are linked to European governance and monitoring structures via common EIF templates.

Conclusions for the EIF:

The discussion on digital transformation highlights, in particular, a need to expand the EIF's recommendations on semantic and technical interoperability, data quality, security, data protection and data portability. These should describe in more concrete terms the requirements that administrative data must meet in order to be usable for automation, data spaces and responsible artificial intelligence.

Question 5 – Proposed changes and improvements

"What changes or improvements would you suggest for the future EIF?"

For the future European Interoperability Framework, priority should be given to five improvements which do not create any new legal obligations but make the voluntary framework significantly more manageable and effective. It is crucial that the EIF not only sets out principles, but also provides administrations, specialist departments and project teams with concrete tools for implementation, procurement, data quality, interfaces, governance and the deployment of new technologies.

1. Implementation toolkit: Interoperability must be translated into concrete project artefacts

The EIF should be supplemented with customisable project templates, role models, templates for data and interface agreements, checklists, test data, minimum security requirements and procurement clauses. This would mean that project teams would not have to reinterpret what interoperability actually means for each new project, but could instead draw on tested and reusable tools.

2. Reference architectures: Recurring administrative processes should not have to be redesigned from scratch every time

The EIF should provide domain-specific reference architectures and reference solutions. Recurring patterns such as register queries, status messages, verification objects, specialist portal interfaces, data set catalogues, secure evaluation environments or operator interfaces should be made available as comprehensible reference patterns. Suitable initial areas of application include police information exchange, migration and register processes, health data, environmental and geodata, mobility and infrastructure data, as well as funding and verification procedures.

3. Benefit and incentive logic: Voluntary interoperability requires demonstrable added value

Interoperability initially entails additional effort, as public authorities must jointly clarify responsibilities, data models, interfaces, data protection issues and operational accountability. This effort will only be borne if the benefits become apparent. A maturity model should therefore not only assess the state of interoperability, but also identify specific risks and benefits: lower integration costs, faster implementation of digital services, better data quality, less manual verification, greater reusability, reduced vendor lock-in and more robust implementation of European requirements.

4. Procurement and governance: Interoperability must be mandatorily factored in before a project begins

The EIF should embed interoperability at an earlier stage in procurement, architectural decisions and national coordination. Tenders should include verifiable requirements for open interfaces, data export, versioning, logging, testability, system replaceability, data portability, authentication, role and rights concepts, as well as clear interface and data responsibilities. Architectural approvals should assess not only functional requirements but also reusability, semantic interoperability, security and data protection design, and operational responsibility. National contact points should play a stronger role as intermediaries between the European framework, national governance and specialist domains.

5. Data, AI and sovereignty: The EIF must enable machine-readable administration

The EIF should be specifically supplemented with support for machine-readable semantics, artificial intelligence and digital sovereignty. What is needed are mapping tools between European, national and domain-specific data models, for example for individuals, organisations, addresses, evidence, events, status, location and time. With regard to artificial intelligence, the EIF should set out minimum requirements for metadata, data quality, subject-matter-expert-verified reference and test data, traceability, logging and model governance. For digital sovereignty, open standards, portable data, interchangeable components, European operational options, open source and realistic migration scenarios should be made assessable.

CONTACT

Werner Achtert
Executive Business Consultant
Public Sector
werner.achtert@msg.group

Björn May
Division Management
Public Sector
bjoern.may@msg.group