DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

Export z Národní architektury eGovernmentu ČR

Obsah

Information Systems Decomposition 3

Information Systems Decomposition

The public authority shall perform and maintain an up-to-date decomposition of information systems or parts of information systems[1] to support decision-making about their long-term management in three independent and mutually combining views, namely:

- functional partitioning, i.e. partitioning into components according to different functions in support of the performance of public administration services and the operation of the public administration body,
- technological division, i.e. division according to the technological platforms used for the design, development and operation of information systems and their components,
- operational division, i.e. division into environments, according to their different uses in the life cycle of information systems and their components.

The public administration shall apply the decomposition of information systems, in particular in the basic documents of long-term management.

Functional decomposition is performed at all layers of the information system architecture, namely by dividing it into application components, technology components and communication components.

In the functional decomposition of information systems, the public administration authority shall use the classification systems according to the reference models of information systems architecture, namely application and technology, issued by the Ministry.

In the technological decomposition of information systems, the public administration authority shall use classification systems according to the reference models of information systems architecture, namely solution architecture and technology architecture, issued by the Ministry.

The operational environment decomposition shall be performed according to the actual life cycle needs of the individual information systems or their components, in particular the environment for

- proof of concept,
- initial testing of platforms or delivered finished solutions,
- development and testing iterations,
- demonstration and validation of development iterations,
- testing the functionality, quality, performance, reliability and integration of development iterations prior to acceptance,
- acceptance, pre-production and production testing,
- operator training, study and practice,
- backup checking, disaster recovery drills and operational archive,
- end-of-service verification, locked system and post-operational archive,
- productive use,
- analysis and verification in a copy of the productive environment.

To meet the needs of integration verification, training, and development, components and environments can be created and integrated with purpose-constrained behavior. Each such environment must be uniquely identifiable and use only its own unique identifiers to access other environments. Changes to data entered through such an environment must be identifiable and its operation must not result in a valid change to the records in the productive agenda record.

When using and providing the services of a purposeful behaviour environment, the administrator shall establish rules for

- the provision of data by the services of the constrained environment in terms of quantity, structure and concealment of real data, especially personal data, through pseudonymisation, anonymisation and randomisation,

- the execution or simulation of transactions and changes to data triggered by the restricted environment which may not be entered into productive databases and registries as valid changes,
- the execution or simulation of the execution of operations and interactions with other integrated systems in such a way that it is evident that they are operations triggered by the operation of a purpose-limited environment,
- the inter-availability of interfaces for the provision of services to the constrained environment, the production environment and other integrated environments for their own and other systems, their identification and the issuance of authentication means.

The operator may, within a framework specified by the administrator, create, operate, and decommission environments for the performance of various subtasks in relation to or across stages of the information system life cycle. In doing so, he/she shall ensure, while respecting the rules specified by the administrator, in particular

- the unambiguous identifiability of the environment, the data acquired and modified by it, the transactions performed and the services used,
- the allocation of identifiers, the management of identity resources allocated to individual environments,
- protection of sensitive data from unwanted disclosure, especially from the production environment,
- protecting the trustworthiness of the production environment and production data.

The measures referred to in the last 2 paragraphs may be part of the design of the information system and may also serve its own development.

[1] A similar decomposition shall also be performed by the public authority for elements of shared infrastructure.