Materiál Ministerstva vnitra

Export z Národní architektury eGovernmentu ČR

Obsah

Need for and cost-effectiveness of information systems

Information systems should be created for a purpose and deliver an effect for a reasonable cost. Efficiency, effectiveness and economy (the so-called 3Es) are defined in Law No. 320/2001 Coll., Audit Standards of the SAO or in Manual of the European Court of Auditors. Authorities are obliged to use assets in accordance with the 3Es and to monitor and evaluate spending in accordance with the 3Es according to Law No. 219/2000 Coll. and 218/2000 Coll. In addition to the Supreme Audit Office (SAO), the Office of the Chief Architect of eGovernment (OHA) also supervises the 3Es and assesses the necessity, feasibility, benefits, and economic and staffing requirements of public administration digitisation projects. It is desirable for authorities to follow management of individual ICT solutions according to methods of ICT management of public administration in the Czech Republic.

The increased risk of non-compliance with efficiency and economy in the case of implementation of public administration digitisation projects results, among other things, from the continuous very rapid development of digital technologies and thus their extremely rapid moral obsolescence and economic depreciation as a practical consequence of the so-called *Moore's Law*. This is what makes it potentially impractical and uneconomical, for example, to acquire any information and communication technologies that will not make adequate use of their computing power, transmission capacity, data storage capacity, high availability or superior level of support even in the next 18 months.

Whether project documents, software or data layout, their use is restricted by copyright law, in particular Act No 121/2000 Coll. In addition to in-house development in the form of employee work, most software is obtained by paying for a licence to use the work. If nobody except the originator or his authorised representative may modify the work, provide additional services to it or link it to other units, change its users, etc., the effective use of the work is blocked and the customer is completely dependent on the arbitrary will of the originator. Such a situation is called vendor lock-in and can lead to wasteful spending. It is not only software that is affected, but also the supply of complex hardware assemblies that limit the subsequent freedom to maintain and expand such equipment, the purchase of consumables and services, as well as the enforcement of service or 'maintenance' fees without the ability to use the equipment after such terms have expired. OHA has written examples of unfavorable contract provisions and recommends that such provisions in licensing agreements be limited as much as possible and preferably replaced with provisions that give the user the broadest possible control over the ICT product. The existence of vendor lock-in or the risk of its occurrence may lead to the unfeasibility of the relevant public administration digitisation projects and thus to their uneconomical and inexpedient preparation due to the violation of the principles of transparency, proportionality, equal treatment and non-discrimination set out in Act No. 134/2016 Coll. and the subsequent imposition of a ban on the performance of the relevant contract by the Office for the Protection of Competition.

Authority Concepts and Strategies

An Information Concept (IC) is a strategic document used to set the direction for the development and management of ICT. The Information Concept is compulsory for every public authority and voluntary for other authorities. An authority's IC is not intended to go in depth, but only to set the direction by which projects will be implemented. At the same

time, it must be regularly updated and approved by the top management. The IC has a compulsory structure and content as laid down in Decree No 529/2006 Coll., beyond which the Authority can of course expand the IC with the necessary information. In addition to the individual IKs, there is a national Information Concept of the Czech Republic (IKČR), which sets out the principles and principles that are further elaborated in its follow-up documents and determine the direction of digitisation of the entire public administration. The legislative process does not always correspond to the real situation, which is unfortunately also reflected in the requirements for the IK, where the decree does not contain the necessary data to comply with the IKČR, so we recommend using knowledge base with texts on the IK and compliance of the IK with the IKČR. The IK of the Office should also be linked to the Service Office Development Strategy, which the Offices have to prepare according to the methodological guideline for quality management in service offices by 30 June 2021.

The Decree No. 529/2006 Coll. also sets out the structure and content of the operational documentation. The operational documentation should describe the functional and technical characteristics of the public administration information system and elaborate on the authorisations and obligations of its administrator, operator and user. It is compulsory for every public administration body, voluntary for other authorities.

Information concept, operational documentation and other required documents are not an unpleasant part of methods of ICT management in public administration. These documents should be considered as an essential part of any organisation that owns ICT. Operational documentation is an integral part of ICT, without which the public administration information system is just a "black box". Operational documentation is therefore mainly to help understand the public administration information system, how to treat it and how to manage it.

Public administration channels

Public administration service channels can be understood as ways or means of communication between a public administration client and a public administration. Through service channels, a digital action can be performed and a digital service can be used. The right to perform a digital act and use a digital service is enshrined in Law No. 12/2020 Authorities should strive to ensure complete electronic submission, through which a citizen can digitally handle his or her entire life situation at any time and from anywhere or through a universal contact point. An overview of the data on public administration services, operations and their service channels is given in the public administration services catalogue.

One of the main service channels is the Citizen's Portal, which is the web portal of the Czech digital public administration and enables centralised access to information and digital services. In order to log in to the login portal, the client/citizen must have a so-called guaranteed electronic identity, i.e. logging in is enabled via a qualified electronic identification system, currently NIA or authentication interface of the Information System of Data Boxes. The citizen portal allows various advanced interconnections (federations) of portals or public administration systems. It is therefore desirable that digital services and actions provided by authorities through their portals are also available on the Citizen Portal. In this way, authorities will support many architectural principles such as P8: One State, P9: Shared Public Services or P11: eGovernment as a Platform. In line with the principle P1: Digital by default authorities must keep other channels open for those who cannot use digital services either by choice or for technical reasons. However, the paper-based or assisted form of the service should be derived from its digital form. An assisted service channel is e.g. Czech Submission Authentication Information National Terminal (Czech POINT). In the area of centralised web portals, e.g. the Entrepreneur's Portal,

which can be seen as an extension of Public Administration Portal, should be created in the future. It is also worth mentioning the unified service channels for civil servants.

In addition to the national portals, there are also territorial portals, typically for a region, municipality, city or urban district. A territory portal may contain, in addition to self-governing services such as the management of local taxes, also delegated services. However, it should not be the case that a delegated service is created only for the territory portal. It is the responsibility of the content manager to create a central environment for handling the delegated services that the territory portal will use but not create. From the point of view of user-friendliness, the possibility of redirection/transition between portals must also be addressed. Such behaviour must be intuitive and non-intrusive.

There are also portals for private data users (PDCs). These can be portals of health service providers, private insurance companies, banks, state-owned enterprises, etc. These portals provide services that can be federated to the Citizen Portal, but only if the SPSU is registered in registry and has the obligation to electronically verify the identity of the client.

Electronic circulation of documents

The performance of government administration is accompanied by the creation of documents, their signing, filing, sending, receiving, shredding, etc. These activities, collectively referred to as document management, are carried out within the framework of the filing service. A number of entities are obliged under Act No 499/2004 Coll. to carry out filing services in electronic form, i.e. through electronic filing systems (eSSL). Detailed technical requirements for the application and business functions of eSSL are set out in national standard for eSSL. Do not overlook the rules for eSSL.

In order for documents to be circulated electronically, obliged entities must ensure that authentication and authorisation elements are attached to the documents produced in digital form and that the authenticity of the documents delivered is verified. Regulation eIDAS provides a consistent legal framework for the use and recognition of electronic signatures and digital seals. And it is the use of electronic signatures, guaranteed electronic signatures and, in particular, qualified electronic signatures, which are legally on a par with handwritten signatures, that enables the efficient circulation of documents with their authenticity guaranteed.

In order to ensure trustworthy, secure and authentic electronic communication between public authorities on the one hand and natural or legal persons on the other hand, as well as between public authorities among themselves, the Ministry of the Interior of the Czech Republic operates the information system of data boxes (ISDS). Sending documents via ISDS not only helps to ensure the strictest conditions required in the framework of cyber security, but also contributes to strengthening trust, simplifying communication and the accuracy of documents between authorities. Documents sent and received via datacoxes in this way have the same legal value for legal and natural persons as if they had been sent in analogue form via a mailroom. ISDS activities are carried out free of charge. Only conversion on request (30 CZK per page) and reissue of access data (200 CZK) are charged. Authorities recommend use ISDS as an integral part of their electronic filing service.

State and local government authorities according to Law No. 134/2016 Coll. may not refuse electronic invoicing issued by the supplier for the performance of a public contract. The National Standard for Electronic Invoicing enables paperless exchange of structured electronic invoices and other documents, their fast processing and portability between

businesses, public administrations and private parties. The electronification of processes over all documents circulating within the authority respects the architectural principles P1: Standard digital and P12: Intrinsically digital only and determines the quality and efficiency of the work of state and local government.

Identification in information systems

Every information system (IS) is accessed by users, so it is necessary to verify their identity, called identity, and set their rights to individual actions. In the area of government services, this authentication needs to be reliable and guaranteed at a HIGH level in accordance with government client identification rules. After all, this often involves handling finances (tax returns), property (land registry) or even sensitive data (health information, social security). Electronic means of identification are used to verify identity, which can be seen as an imaginary key to open the identification gate.

Currently, an ID card with an activated contact electronic chip, NIA ID, eGovernment mobile key, my ID, bank ID or first certification authority can be used as identification means. The Information System for Data Boxes (ISDS) allowed the use of the identity space of data boxes for logging into custom solutions - typically portals. This method of identification and authentication of the public administration client was enabled only until July 2020, when the transitional provision of Law No. 250/2017 Coll., which introduced the obligation to use the National Identity Authority (NIA) system, expired. In the case of remote identification and authentication through the NIA, the natural person is uniquely identified by a meaningless directional identifier (BSI), which can be converted through the information system of basic registers (ISZR) into an agency identifier of the natural person (AIFO). By using electronic identification, authorities contribute to the fulfilment of Objectives 1.3, 1.6, 2.7 and 3.6 of the Information Strategy and comply with the architectural principles P8: One State and P11: eGovernment as a Platform.

Thanks to Regulation eIDAS, the electronic identity of persons is recognised within the EU, which supports the architectural principles P5: Cross-border access as standard and P6: Interoperability as standard. In practice, this means that any citizen of an EU Member State has the right to legally prove his/her electronic identity anywhere within the EU using a notified identity means of the home state. Thus, for example, a citizen of the Czech Republic can prove his/her eObčanka (eOP) with a notified electronic means in Denmark and use services through their portal. Information systems used within the EU should therefore be able to verify the identity of the foreign national via the so-called eIDAS node and follow other rules for NIA.

Civil servants and other public administration staff should preferably use the Unified Identity Space (UIS) and the Catalogue of Authentication and Authorisation Services (KAAS) for their identification. If the IS is not connected to the JIP/KAAS, the subject administrator together with the IS operator is responsible for the correct access settings and authentication is performed in the local identification system or directly in the IS. In order to use the JIP/KAAS interface, the IS must be connected to the central service point (CMS).

Structured data in ISVS, data pools and data sharing

Every information system (IS) contains data and information. Whether it is agenda or non-agenda data, it is always true that data represents valuable information value. In order to be able to work with data as efficiently as possible, the authority owning the IS must ensure that all data can be accessed in an open and machine-readable format, at no

additional cost and with the ability to manipulate the data freely. This is a prerequisite not only for the efficient performance of public administration, but also for the publication of open data.

Not sure how to make your IS ready for open data publishing? Read whitepaper OHA. In order to be open data according to Law No. 106/1999 Coll., the authority must register it in the National Catalogue of Open Data (NKOD), where citizens, companies and other authorities can find the data. By publishing new datasets or improving existing publications, authorities contribute to the fulfilment of *Objectives 1.5 and 5.10 of the Czech Information Concept* and comply with the architectural principles *P4: Openness and transparency* and *P13: Open data as a standard*. You can learn more about open data at data.gov.cz and opendata.gov.cz.

Of course, in the area of data, it is also important to think about data protection. We recommend to follow rules of subject registration and to use the so-called Agenda Identifier of the Individual (AIFO), which ensures pseudonymisation in the context of public administration. The birth number should not be used as an identifier as it creates the possibility of easy misuse of data. Do not overlook principles of pseudonymisation.

One of the problems in the area of data is data quality. In this area, we recommend implementing input control mechanisms, describing the structure of the data, e.g. using semantic models, and using available open formal standards (OFNs), which contribute to data standardization and interoperability.

In line with the principles of eGovernment, the introduction of a public data repository is planned as one of the tools for data access, alongside open data and the linked data repository. With this tool, public authorities will exchange public data with a guaranteed guarantee, e.g. in a first phase, e.g. codebooks.

Public Administration Interface

The Government Reference Interface allows multiple entities to access given data simultaneously. Within this interface, data from the basic registers, i.e. Register of Population (ROB), Register of Persons (ROS), Register of Territorial Identification, Addresses and Immovable Property (RÚIAN) and Register of Rights and Obligations (RPP) can be used via the Information System of Basic Registers. The protection of personal data in the basic registers is ensured by the Agency Identifier of Natural Persons (AIFO) converter, which makes it impossible to search for data on a natural person in another agency if one identifier is known. The Basic registries are not used to directly perform a specific agenda, but to supply guaranteed data to entities that have the right to use the data for specific agendas. Thus, they are now an essential support tool for the performance of most specific agendas in the public administration in the Czech Republic.

Another component of the public administration reference interface is the eGovernment On-Line Service Bus / Information Shared Service System (eGSB/ISSS). Through eGSB/ISSS, authorities can exchange data held in agency IS on the basis of authorisations. The administrator of the agency IS that publishes the data creates a context through which it provides the defined data. It is recommended that only one comprehensive context is published from each IS, whose sub-contexts can be drawn upon by the authorities according to their authorisation. eGSB is at the same time linked directly to the ISZR, thus ensuring communication about persons with a link to the AIFO of the respective agenda. The use of the eGSB for the use of data between the agency ISs and at the same time for the provision of outputs to the subjects of law by the authority not only ensures the fulfilment of the legislative obligation, but also brings a clear increase in transparency and, thanks to the communication through the Central Service

Point (CMS), also the security of this exchange. The publishing body will certainly appreciate other advantages of eGSB/ISSS, e.g. it does not have to verify the source of the query (Agenda, Public Authority, Information System or directly the interviewer), it is not responsible for the identification of the data subject (the interviewer is responsible for the exact identification of the AIFO), it does not have to maintain one or more interfaces towards a large number of interrogating information systems or even to the public Internet (there is only one publishing interface with cyber protection in the CMS). At the same time, the cost of providing this activity will be reduced.

The ISZR and eGSB/ISSS together form the Interconnected Data Pool, the development of which is *objective 5.9 of the Czech Information Concept* and supports a number of architectural principles, e.g. *P2: The "only once" principle*, *P6: Interoperability as a standard*, *P8: One State*, *P11: eGovernment as a platform* or *P16: Consolidation and interconnection of public administration information systems*. Do not overlook global architecture of PPDF. It is desirable that any IS that maintains data on individuals or exchanges such data with other agency IS outside the ministry is linked to a reference interface. Prerequisites for connection to the reference interface are registration of the IS in the ISVS register, keeping up-to-date information on the agenda in the RPP and ensuring connectivity to the CMS.

Shared Agenda Information Systems

In addition to the central services that are the responsibility of the state, there are a number of shared information systems (IS) that are the responsibility of the relevant authorities, although they cover the whole of public administration. The National Architecture Plan distinguishes between shared agency ISs under delegated competence (e.g. Trade Register, Drivers' Register and Motor Vehicle Register) and shared agency ISs for the autonomous competence of local governments. In addition, there are shared operational IS, which include e.g. the Integrated Information System of the Treasury (IISSP), the Central Register of Administrative Buildings (CRAB), the CEDR Information System, MS2014+, the Register of Contracts and the National Electronic Tool (NEN).

There are no specific rules in these areas yet, but the National Architecture Plan gives room for their creation. It is desirable that the authorities in charge of shared agenda and operational IS create rules that other authorities should follow. These include, for example, user rules (i.e. how IS users should behave), system rules (i.e. how other authorities' IS can be linked to the IS) and semantic rules (i.e. what data other authorities should enter into the shared IS).

Public administration communication infrastructure

The Communication Infrastructure for Public Administration (KIVS)/Central Service Point (CMS) can be called a private network for the performance of public administration by all entities - i.e. both public administration bodies (PABs) and private data users (PDCs). This network primarily provides secure interconnection of public administration information systems (PIS) or private data use systems (PUDS) operating in public administration agencies with other PIS, but also, for example, secure access to the public Internet. With KIVS/CMS, access to eGovernment services is ensured with defined security and SLA parameters. In accordance with sub-objective 3.5 of the Information Concept of the Czech Republic, KIVS/CMS is being conceptually developed. The PSCs are obliged to provide ISVS services in accordance with Law No. 365/2000 Coll. through KIVS/CMS, and rules for KIVS/CMS are related to this. By using KIVS/CMS, the OVS fulfils the architectural principles *P8: One State* and *P11: eGovernment as a platform*. The CMS also provides

access to e.g. linked data pool. Services overview of the CMS is regularly updated.

KIVS/CMS therefore offers the following for individual OVS:

- Secure and reliable access to the application services of individual CMSs
- Secure and reliable publication of the application services of individual CMSs
- Secure access to the Internet
- Secure access to mail services on the Internet
- Provides a secure network environment to ensure interoperability within the EU
- Enables secure access to ISVS application services intended for VS end-clients from the Internet.

The OVS and the SPS access the connected data pool exclusively via the CMS in one of four possible ways:

1. Through Regional Networks (currently in the Vysočina, Pilsen, Karlovy Vary, Zlín and partly Pardubice regions + others if built).
2. Through metropolitan networks of district towns (currently about 77 district towns).
3. Through the Communication Infrastructure of Public Administration (CIPA) using commercial offers competed through the Ministry of Interior or for example Integrated Telecommunication Networks (ITS).
4. Via the public internet, using a secure VPN SSL or VPN IPSec tunnel.

If the Authority wishes to use a public KIVS operator, i.e. tender through the central contracting authority of the Home Office, it is necessary to define the requirements according to catalogue sheets and then implement the purchase in a dynamic purchasing system. CMS services can also be obtained via National Data Centres.

Cloud Services

Progress on Cloud computing remains open in light of the recent CJEU decision in Case C-311/18.

The Commission's implementing decision of 12 July 2016 under Directive 95/46/EC of the European Parliament and of the Council on the adequate level of protection provided by the EU-US Privacy Shield has been declared invalid by the CJEU in Case C-311/18 Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (so-called Schrems II) of 16 July 2020. It is therefore no longer possible to transfer personal data to the US under the Privacy Shield.

See https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=43874&n=uoou%2Dk%2Ddopadum%2Dzruseni%2Dstitu%2Dsoukromi%2Deu%2Dusa%2Dna%2Dspravce for more information.