Materiál Ministerstva vnitra

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Export z Národní architektury eGovernmentu ČR

Obsah

Global architecture of the interconnected data pool

The Global interconnected data fund Architecture is an annex of the NAP itself and is elaborated in expanding knowledge base.

Executive Summary

Document Objectives

The Global Architecture of the Linked Data Pool of Public Administration of the Czech Republic presents a description of the Linked Data Pool, the rules of work of individual roles (editor, publisher, reader, manager, auditor) and the rules of providing data on subjects and objects in public administration information systems.

Due to the fact that this is a strategic document, not all the rules and requirements for the linked data pool may be in line with the current technical and procedural state of public administration information systems and the legislation in force. The aim of the document is to create a binding strategic framework that will be further developed in individual areas (information systems architecture, legislative framework).

High-Level view of the Linked Data Fund

The Linked Data Fund is being developed:

- **Agenda information systems**, which, by virtue of the execution of agendas, ensure the creation of data on subjects or objects of law (the data are created here) - hereinafter referred to as "authoritative data originator".
- **Basic registers ROB and ROS**, which, as specialised Agenda Information Systems, provide reference data on subjects of law and ensure unambiguous linking of data to the subject of law.
- **Basic register RÚIAN**, which as a specialised Agenda Information System provides unambiguous linking of data to territorial elements and addresses.
- **The ORG converter,** which ensures the conversion of the Basic Identifier of the natural person and the split electronic identity in the individual agendas (Agenda Identifier of the natural person).
- **Registry of Rights and Obligations - provides** reference data for the management and administration of the linked data pool.
- **Reference Interface** - a shared and secure interface to public administration information systems accessible via the Central Service Point.
- **Basic Registry Information System and Shared Service Information System -** part of the reference interface that provides application access to reference and agency information system data

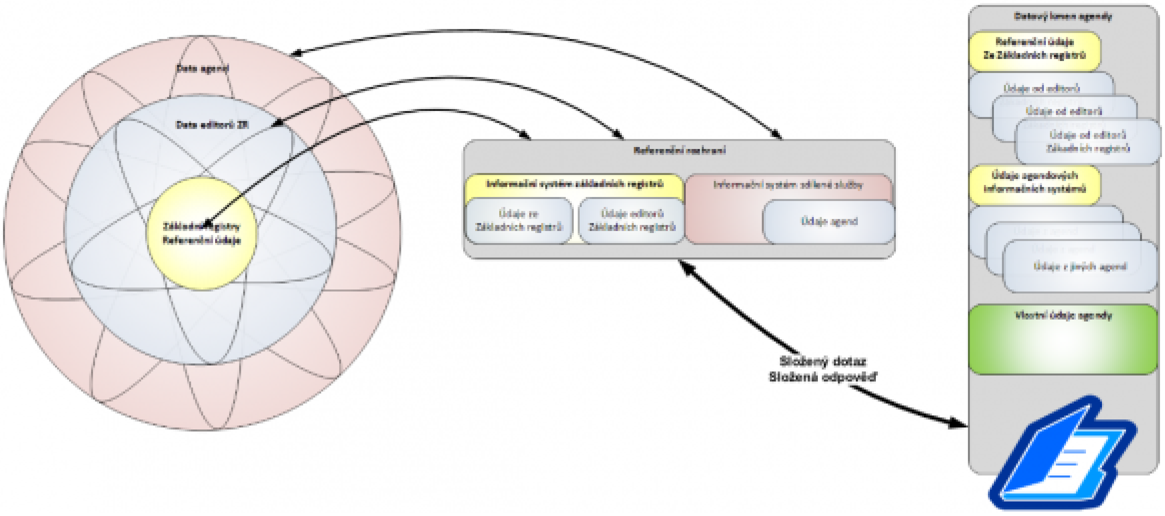
> The linked data pool is therefore used for the exchange of data on subjects and objects of law.

The Linked Public Administration Data Pool creates a complete data base that contains all data on subjects or objects of law that are held in public administration information systems. However, the merging of data on a single subject cannot be carried out without the necessary authorisations of the individual agencies, and in particular the personal data of natural persons are highly secured against unauthorised merging.

The individual roles of the Agency Information Systems for activities in the linked data pool are:

- **Publisher** - Agenda Information Systems providing data on identified subjects or objects.
- **Reader -** Agency Information Systems and designated private data user information systems.
- **Reference interfaces** providing communication between readers and publishers.

Figure 1: Data distribution and exchange scheme


Data agend
Data editorů ZR
Základní registry
Referenční údaje
Referenční rozhraní
Informační systém základních registrů
Údaje ze Základních registrů
Údaje editorů Základních registrů
Informační systém sdílené služby
Údaje agend
Složený dotaz
Složená odpověď
Datový kmen agendy
Referenční údaje Ze Základních registrů
Údaje od editorů
Údaje od editorů
Údaje od editorů Základních registrů
Údaje agendových informačních systémů
Údaje z jiných agend
Vlastní údaje agendy

Within each agenda, the following types of data are maintained about the entities in each role (context) in terms of the linked data pool:

- Reference data from basic registers.
- Data from other agendas (Agenda Information Systems).
- Data created within the framework of the agenda activity - only these data can be provided by the agenda to the linked data pool as data of the agenda information system.

It should be emphasised that reference data and data from agency information systems can only be provided within the linked data pool on entities that exist or have existed (e.g. deceased persons for a period of time before the deletion of the registration) in the basic registers. For other persons, there is no such unambiguous link to the entry in the basic registers and therefore the primary condition of unambiguous identification of the person about whom the data are transmitted is not ensured, and therefore the data are always of an informative nature only and it is not the case that the public authority using the data does not have to verify their validity.

The interconnected public administration data pool provides the highest benefit to the subjects of law, as it ensures that the public administration will work with their up-to-date data and that individual authorities/agencies will not repeatedly require citizens or legal entities to prove their data.

A significant benefit for public administration employees is precisely the status of *correctness* of the data on legal entities that they obtain through the linked data pool. This means that the data is guaranteed by the agencies in which it is created and the recipient does not have to carry out complex verification of the data necessary for the performance of their agenda.

Background and rules of the Linked Data Pool

Summary of functionality

The primary means of securing individuals' personal data is through the use of split identity, where an individual is held in each Agency Information System with a unique electronic identification using an AIFO (Agency Identifier of the Individual), which varies between Agencies. The converter of these AIFOs (ORG) is managed by the Data Protection Authority and is only available through the Information System of Basic Registers (ISZR). Therefore, without the cooperation of the ORG converter and the ISZR, it is not possible to merge data on one natural person from different agencies (including the basic registers of the Register of Population and the Register of Persons).

The management and description of the entire interconnected data pool is stored in the Register of Rights and Obligations, which contains a description of all parts of the interconnected data pool down to the technical details, enabling unambiguous implementation and management of all functionality, including the orchestration map of data folding.

This information is then used by the individual components of the Linked Data Pool to manage the processes and permissions for the transfer and use of data.

The Rights and Obligations Register is, amongst other things, the repository of all the information required for the transfer of data within the Linked Data Pool. It contains data on the individual process participants (Agency Information Systems, Public Authorities and Private Users), the structure of the data to be transferred, its representation (forms) and the structures for managing data access permissions. All participants in the linked data pool are obliged to follow these data.

Transmission of data

The transfer of Linked Data Pool data may be made on the basis of **direct** or **indirect** linkage

- **Direct linkage** - direct communication between different public administration information systems. In this communication, data are exchanged **without the participation** of the ISZR or ISSS**.** In the case of direct link communication on law subjects **<u>must</u>** not be transmitted by AIFO and the communication **<u>must</u>** be supplemented by indirect communication via the ISZR or ISSS, in which, in addition to the translation of the AIFO, the list of data that are transmitted in the direct link is also supplemented (in order to record this transmission).
- **Direct linkage** - transmission of data via ISZR and ISSS. When using this link, the link to the basic registers (verification of the existence of the entity in the basic registers and translation of the AIFO) and the recording of the list of data transferred is ensured. The indirect link also facilitates the work of the publisher, who does not have to create and maintain his own interface according to the PPDF rules.

The Rights and Obligations Register contains the control data for data transfer, including access permissions and technical details of individual components and data.

It should be emphasised that the preferred approach is to use <u>indirect linkage</u>, i.e. use of the ISZR and ISSS. Direct linkage can only be used when transferring large volumes of data on entities (e.g. periodic statements) and then only until indirect linkage via ISSS is assured. The direct link can still be used for the transmission of data on objects without a link to subjects.

Obligations of the publisher

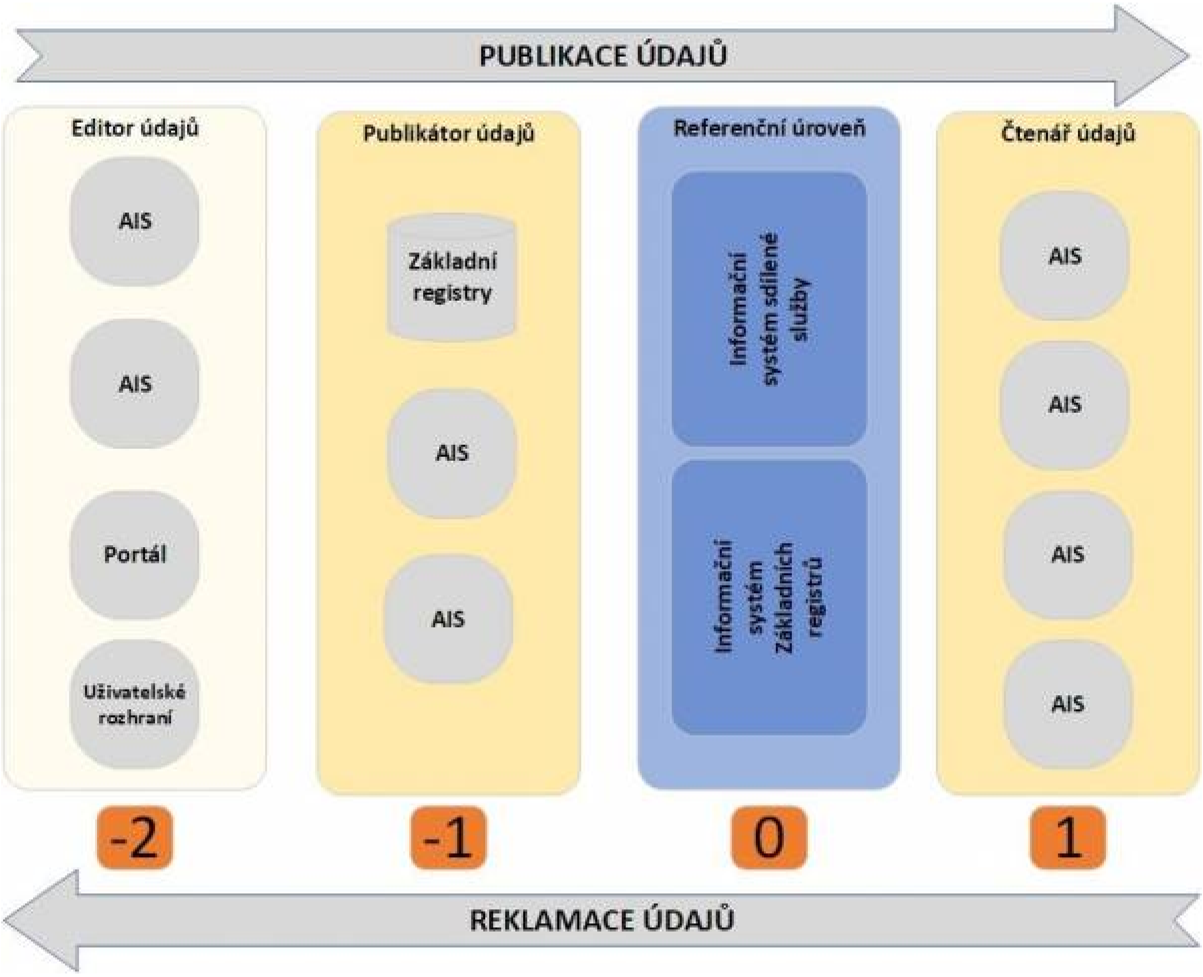
The publisher must provide the following functionality:

- The output of data about an identified subject in an identified role (context) in accordance with the permissions of the reader.

- Identification of a subject according to a given set of data submitted by the reader about that subject in a given role (context).
- A record of all requests and responses (log) including data that is protected against unauthorized access and use. This record shall be provided with technical means (transaction identifiers) to ensure that records are linked across the entire linked data pool. The same obligation also applies to the reader and, consequently, to each ISVS according to the Decree on Act 365/2000, in particular the Decree on the reference interface.
- Means for receiving data complaints in accordance with the legal rules of the agenda
- Means for transmitting information on changes to the data of registered entities
- Means for technical verification of the availability of the publisher's services (probe).

The exchange of data must always follow the logic expressed in the following diagram.

Figure 2: Data exchange schema



This schema, with the necessary simplification, lays down the rules for creating and sharing data and for its subsequent maintenance by means of complaints.

The responsibilities of the publisher must be ensured by the subject administrator in cooperation with the technical administrator of the information system(s), if any, that ensure the execution of the agenda. It is emphasised below whether the information is intended primarily for the substantive administrator of the agenda or the technical administrator of the information systems.

Operational rules

This section summarizes the operational rules on the linked data pool, which are described in more detail in the following text.

A necessary condition for ensuring *the correctness*/ of data and the use of the linked data pool is that the individual public authorities publish data from their agendas (agency information systems) properly to the linked data pool. It should be noted here that by publishing data from their information systems, the agenda manager immediately gains the following advantages:

- They do not need to build and maintain communication interfaces to different entities (providing a direct link), communication with the central components of the reference interface (indirect link) is sufficient for the purpose.
- It does not need to maintain and manage authentication of communication partners, reader data (public authority, agenda, Agenda Information System, etc.) is authenticated by central components and trusted.
- It does not have to manage the access authorisation system. It obtains the authorisation data from the Register of Rights and Obligations.

It is therefore in the interest of all Agency Administrators to maximise the speed of publication of Agency Information System data within the linked data pool.

Process Background

The Linked Data Pool ensures that public administrations processes work with up-to-date data on subjects and objects that are **correct**. The word correct means that the authoritative originator (the editor of the agenda providing the data or the editor of the reference data in the basic registers) confirms its correctness to the best of his knowledge.

Therefore, the data obtained from the linked data pool does not need to be verified by the recipient. A situation may arise where the authoritative originator of the data has doubts about the correctness of the data (handling a complaint), then the data is marked as incorrect by this originator. Conversely, the recipient of the data may discover facts in the course of its activities that are inconsistent with the data provided, then it initiates the complaint process, i.e. it notifies the originator of this doubt in the form of a data complaint.

The subject of the right, natural or legal person, then does not have to prove the accuracy of the data that can be obtained from the linked data pool when contacting the public administration.

The administrator of the AIS maintains the data pool of this AIS in an up-to-date form by using the processes of notification of changes to the data on the linked data pool and the user of the AIS is therefore assured that he is working with the correct data (in the sense mentioned above). From the point of view of the AIS user (official), this is therefore a major increase in efficiency and certainty in his work.

The data from the linked data pool is provided from one agency to another agency via the respective agency information systems. This process is done in the background through a reference interface and does not place any burden on the AIS user.

The second way of using the data is through a standard form of data release request (even bulk data such as a list of changes over a certain period). This form process is handled by the Forms Agency Information System (FAIS), which provides the interface between the Data Boxes (request and output) and the Linked Public Administration Data Pool (FAIS uses the services of the reference interface to handle the request).

In the following chapters of this document, the individual processes are described in detail with the addition of the required architectural and technical standards.

Technical background

The interconnected public administration data pool serves primarily to increase the efficiency of public administration performance support in terms of information systems support. Basic background of the Linked Data Pool:

- Each subject or object of law appears in information systems in a role (context) expressed in legislation (e.g. Citizen, Vehicle Owner, Patient, etc.). One agenda may contain several roles (contexts) for a given type of subject (natural person, natural person doing business, legal entity), thus differentiating the scope of data kept on a given subject. Similarly with law objects. Each context is defined by a unique code in the Register of Rights and Obligations.
- Data on subjects or objects of law "arise" uniquely
    - The data maintained on the subject or object in the information systems supporting the execution of the agenda (Agenda Information System according to Act 111/2009 Coll. on Basic Registers) is defined in the relevant laws governing the execution of the agenda. Thus, the law determines what data is kept in the agenda information system about a given subject of law in the relevant role (context). Similarly for the objects of law. The agenda notifier is obliged to include this list in the Register of Rights and Obligations.
- Each entry is defined by a unique code in the Register of Rights and Obligations and there is a unique location from where it is provided to the linked data pool. The data provided in this way is marked in the agenda declaration as 'reference' in the sense of 'guaranteed' (either a reference from the basic registers or data from the agenda information system). The purpose of the marking as reference is that the public authority can use this data 'without verifying its correctness' within the meaning of the Basic Registers Act for data from the basic registers and individual laws regulating the execution of agendas. The data that already exists about the right holder in the linked data pool does not need to be proven by the right holder.
    - Each reader of data from the linked data pool must ensure that the subject or object for which the data is drawn is identified. Thus, the agenda providing the specific data is not responsible for correctly identifying the data subject, but relies on the identification provided by the reader as part of the query.
    - A reader must not provide back data retrieved from a linked data pool on the basis that it is providing it as guaranteed data, i.e. data from its agency information system (it may only ever provide it as informative data).
    - Reference data and data of the agency information system (within the meaning of the Basic Registers Act) may only be provided on subjects of law that are or have been entered in the basic registers of the Register of Population and the Register of Persons (i.e. there is an AIFO/AIFO or ID number assigned to them according to the Basic Registers Act). Data of agency information systems on other subjects of law (without a link to an AIFO or ID number) may only be provided as informative data on the basis of identification of the subject according to the data.
- Data can be provided within the linked data pool only through the reference interface (§ 2(j) of Act No. 365/2000 Coll. on public administration information systems). The reference interface is mainly provided by
    - Identity of the source and the reader - each information system is uniquely identifiable by means of an SSL certificate issued by the Certification Authority of the Basic Registers Administration.
    - Privacy - all data exchange is carried out in a closed communication environment.
    - Confidentiality - all management data is stored in the Register of Rights and Obligations, neither the source of the data nor the identity of the data reader can be compromised.
    - Auditability - The Reference Interface stores operational data to ensure that communications are auditable.
    - Unquestionability - Rules are set to ensure the unquestionability and provability of the data transmitted (in terms of its transmission and origin, not in terms of its factual correctness, the latter must be ensured legislatively when the data is created).
    - The reference interface is drawn exclusively through the Central Service Point (CMS).

The above basic rules ensure that, throughout the linked data pool, it is always unquestionably clear who is the originator of the data, about which specific entity the data are transmitted, what data are transmitted (including their referential status) and who is the recipient of the data. Due to the logical imprecision of the descriptive names of individual data (e.g. the term 'name' can be seen as a plain name, first names, full name without titles, full name with titles, etc.), each data is listed in the Register of Rights and Obligations under a unique identifier so that confusion cannot occur based on a misinterpretation of the name.

The Global Architecture of the Linked Data Pool also includes the definition of operational rules for the individual parts of the Linked Data Pool to unify the requirements for these individual parts.

Agency Information System Administrator

Each Agency Information System Administrator, in collaboration with the subject matter administrators of the Agencies it supports, must take the following steps:

- Conduct a basic analysis of the required and stored agenda data and divide it into:
    - Reference data from basic registers,
    - Data originating from other agendas (although not currently drawn from these agendas),
    - Data generated by the activities of the agenda it is performing.
- Make a technical connection to the ISZR and ISSS, if not already done so, in the role of reader. Ensure technical conditions such as transaction logging.
- Identify its entire data trunk. The result of the identification for a natural person is the acquisition of an AIFO, the result of the identification for a legal person (including a natural person doing business) is an ID number.
- For reference data and data from other agency information systems, update the data from the linked data pool and start receiving notifications of data changes.
- Prepare the publication of the context/contexts "subject data" in full for each context (legal status of the legal entity in the agenda) and publish this context on ISSS:
    - The right holder has access to the full context,
    - Other agendas request access to individual parts/data via RPP.
- Provide data change notification services so that readers can update their data trunks.

It cannot be expected that these steps will be completed for all public administration information systems in the short term, however it is in the interest of all AIS administrators to take these steps and then gradually retrieve data from other AIS. These steps **are absolutely necessary** in order to fulfil the strategy of the interconnected data pool and the synergy and activity of all substantive and technical administrators of agencies and AIS is absolutely necessary.

Right holder - natural person

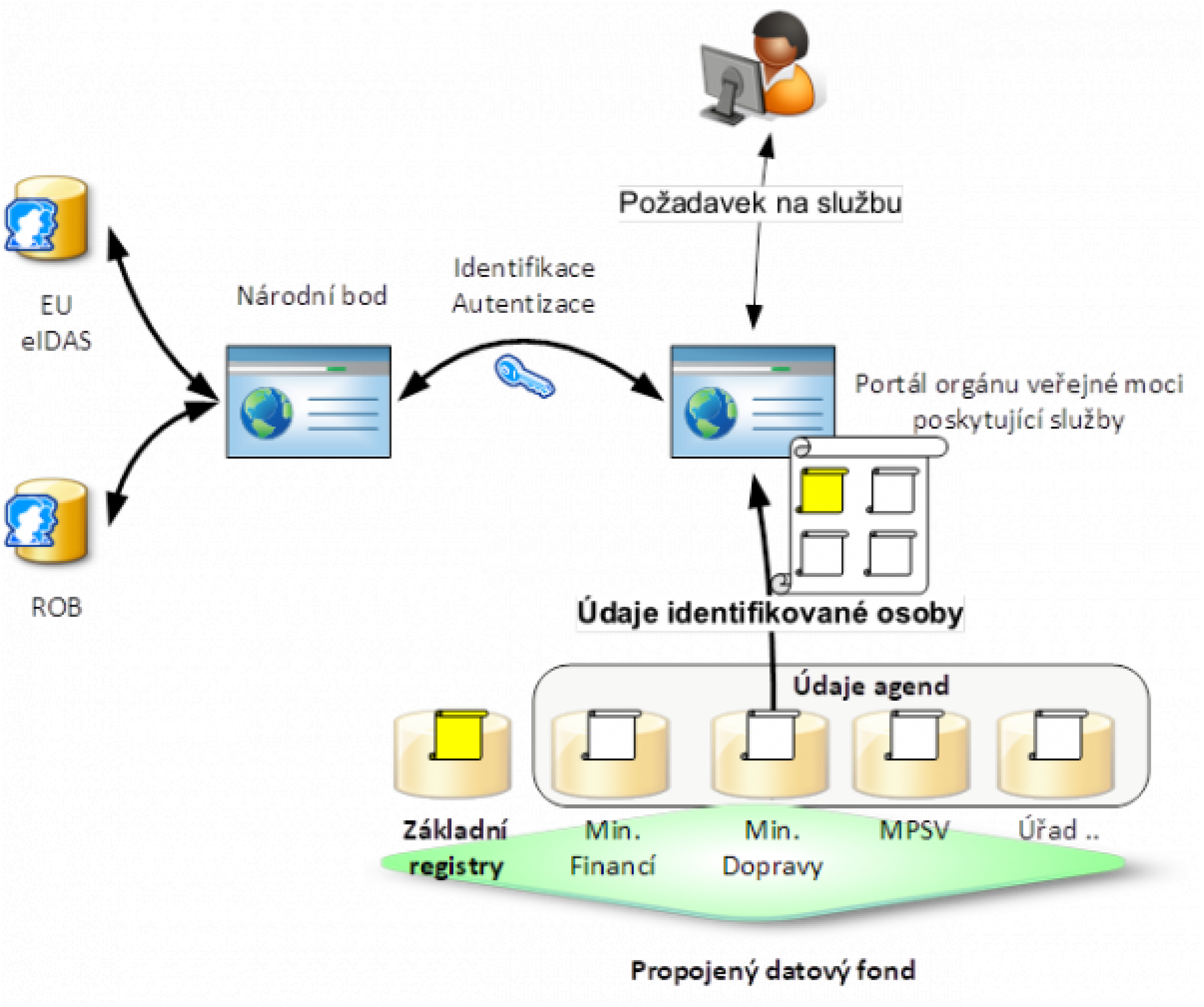
The natural person benefits from the existence of the Linked Data Pool without any action on his/her part. If individual agency and agency information system administrators work on the linked data pool strategy according to the above rules, they will not require the right holder to provide evidence of facts that are already available through the PPDF, thus significantly reducing the burden on individuals and legal entities.

However, if an individual wants to take an active role, which is a welcome approach, then the following steps are recommended for full use and exploitation of the linked data pool environment by the public administration:

- **Establishment of a means of remote identification and authentication** - this will allow the individual to view the data held on them in the individual agency/agency information systems. The data obtained in this way is primarily used to ensure that the public administration is working with the correct data. Otherwise, the right holder can immediately reclaim the data and ensure that the public administration is working with the correct data.
- **Establishment of a data box of a natural person - allows** sending and receiving documents between the public administration and that person. This process fulfils all the requirements of personal submission or receipt of documents and is a necessary condition for the data box holder to be able to communicate with the public administration in a trusted and secure remote manner.

An individual equipped with a remote identification and authentication device will be able to fully benefit from all digital eGovernment services.

Figure 3: Illustrative diagram of the use of digital eGovernment services by natural persons



Subject of the law - legal entity and natural person in business

Many legal entities and self-employed persons already have a data box. For legal entities registered in the Commercial Register or established by law, as well as for some types of natural persons (e.g. lawyers), a data box is established directly by Act No. 300/2008 Coll. on electronic acts and authorised conversion of documents. For legal entities and natural persons engaged in business, whether they have a data box compulsorily or not, the same recommendation applies as for natural persons, i.e. the universal establishment of a data box to ensure trustworthy and free communication with the public administration.

By its nature, a legal person can never act 'alone', but only through a natural person who is authorised to do so. It is therefore in the interest of all legal persons to:

- **To establish a means of remote identification and authentication for all natural persons who can act on its behalf.**
- **Verifying that the basic mandates (i.e. the authority of a person to act on behalf of another person) for actions recorded in the Register of Persons are valid -** otherwise, raising a complaint with the editor of that data to seek redress.
- **Require each agenda manager** to provide an electronic mandate register where an authorised person according to the Register of Persons can authorise a specified individual to carry out relevant actions.

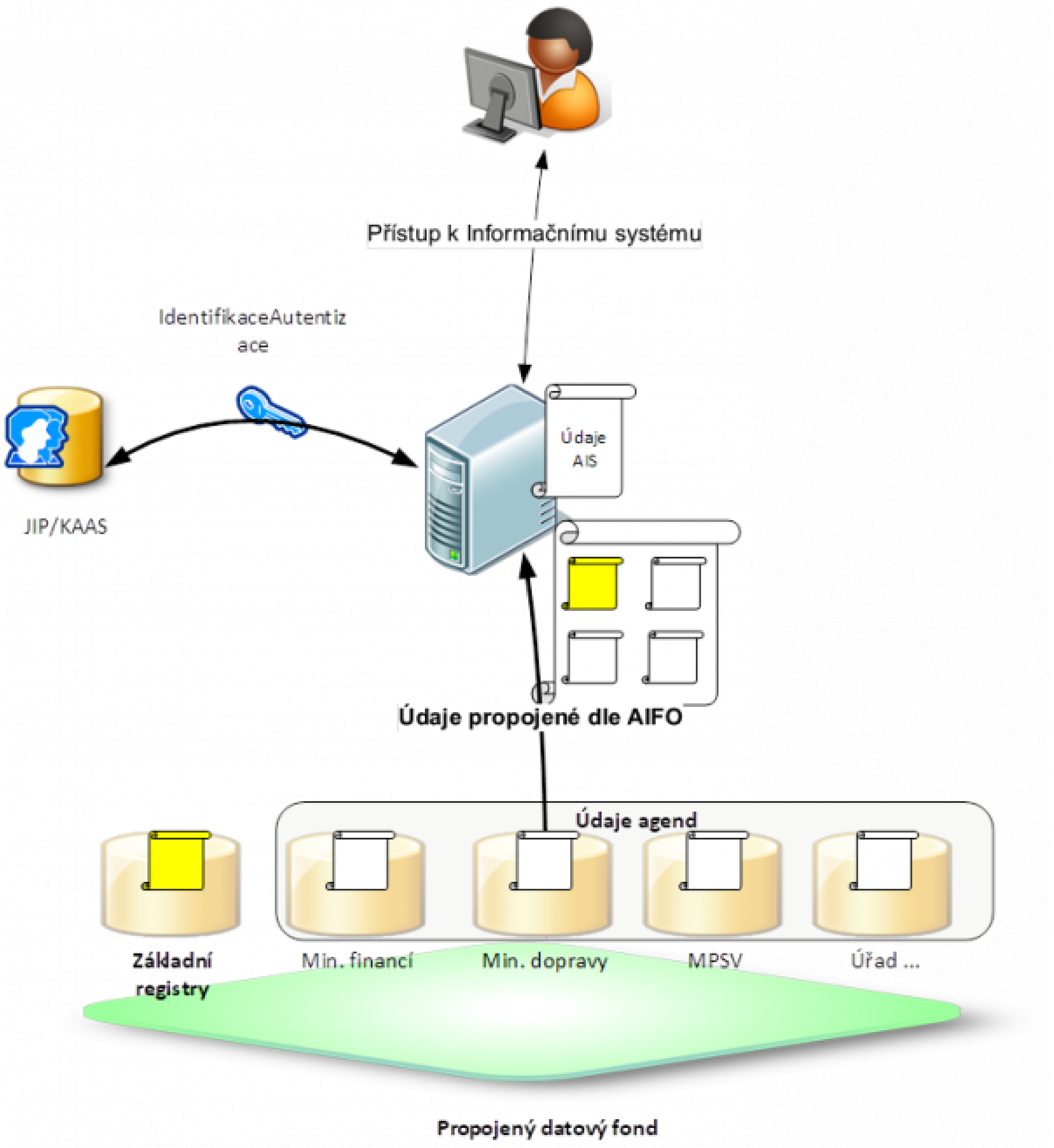
The basis is therefore again remote identification and authentication of the natural person and the maintenance of a link for that natural person to perform acts on behalf of the legal entity in the given agenda. In the Register of Persons, basic mandates are kept as reference data, i.e. mandates resulting from a position such as the statutory body of a legal person. Other mandates, typically mandates arising from a representation agreement (based on a power of attorney) or from a status not registered in the ROS (e.g. an employee in a certain job title) cannot be kept centrally and must be kept in the individual AIS according to the rules of the agendas they perform.

Official - AIS user

From the point of view of the AIS user, there must be no increased requirements. The retrieval of the necessary data from the linked data pool is handled by the AIS with which it is working, in the background, and the data retrieved from the PPDF is displayed to the AIS user with an indication that it is actual reference data or data from other AISs retrieved via the PPDF and therefore does not need to be further verified.

If the AIS user, in the course of his/her activities, finds that the submitted data is not in accordance with the reality, then he/she has to use the data complaint process. This process must be supported by the agenda manager, ideally directly in the AIS in which the user is working.

Figure 4: Illustrative diagram of the use of Linked Data data from a clerk's perspective



Technical Administrator of the Agenda Information System

The AIS Technical Administrator provides the technical link to the PPDF and the connection to all data exchange support services (i.e. not only reading but also receiving change notifications, updating data, etc.).

An important activity is keeping the AIS data pool up to date. For this process, it mandatorily registers in the ORG those AIFOs that are kept in the agenda for receiving notifications of data changes and similarly de-registers AIFOs that are no longer kept in the production environment (transferred to the archive) and thus there is no longer a need to update data on these persons. The updating process is carried out regularly in accordance with the working procedures issued by the Administration of the basic registers.

The updating of data for a longer period of time is carried out **only** in the event of a data breach (restoration from backup, etc.). Repeated reading of data change notifications and updates over a long period of time places a disproportionate burden on both the reference interface and the data source (basic registers and AIS).

In cooperation with the subject matter manager, the agenda manager addresses the identification of the data stem on natural persons (obtaining the AIFO) so that subsequent data maintenance can be carried out by communication according to the AIFO.

Re-identification of the same person according to the data without storing the AIFO in the agenda is an unacceptable waste of the reference interface and data resources.

Description of the Linked Data Pool

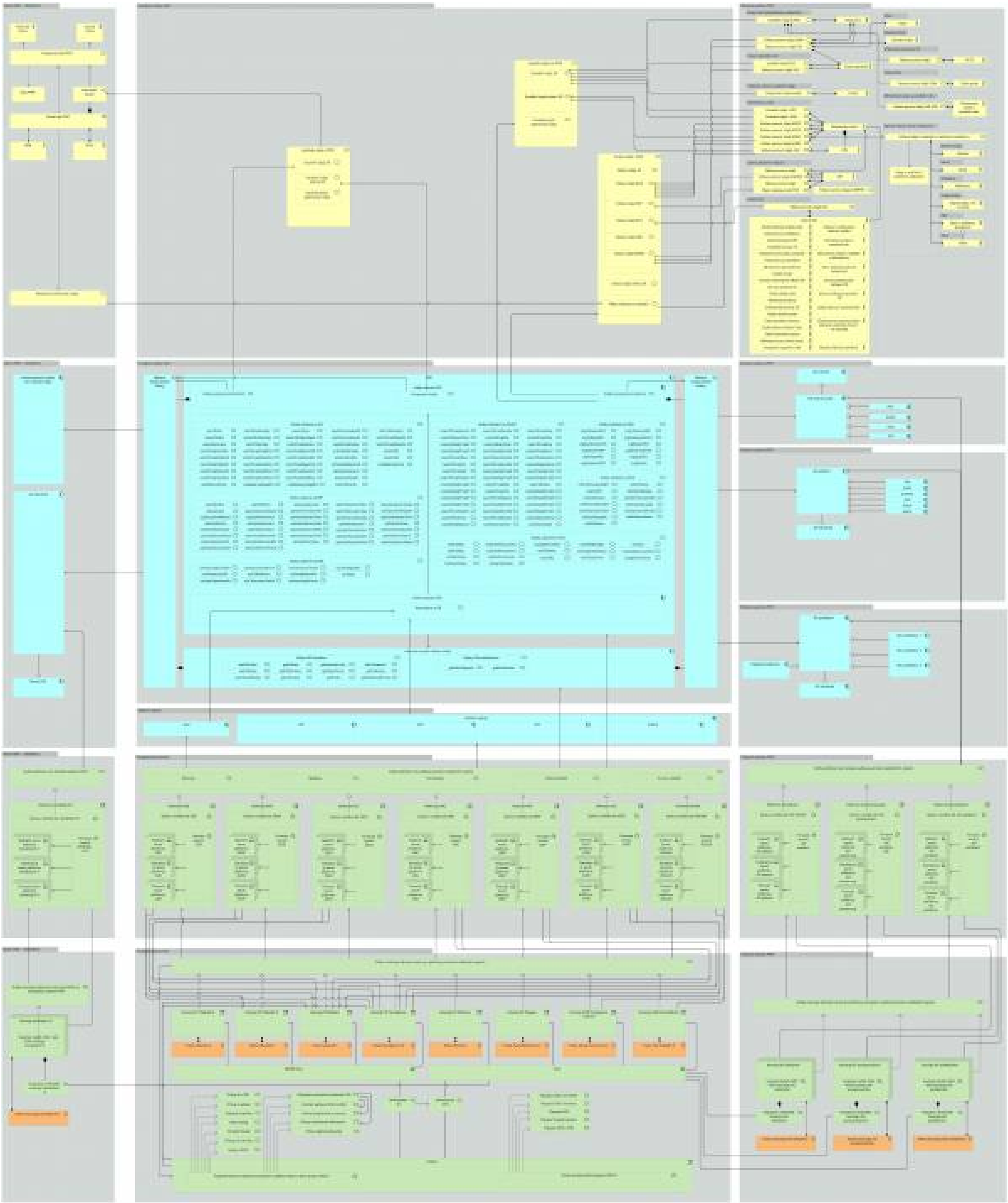
Architectural views of PPDF

Overall view of PPDF in terms of its components, users and technologies

The following figure, or rather architectural diagram, shows the future state of the Linked Data Pool in terms of its components, services, actors, HW and SW technologies and physical interconnection. It is therefore a comprehensive view through all layers of the so-called four-layer architecture of the Czech eGovernment in accordance with the National Architectural Framework.

On the left side are the PPDF clients with their systems and technologies they use to deliver services to the end user. On the right are PPDF sources or editors and publishers with their systems and technologies. In the middle are the PPDF systems and technologies.

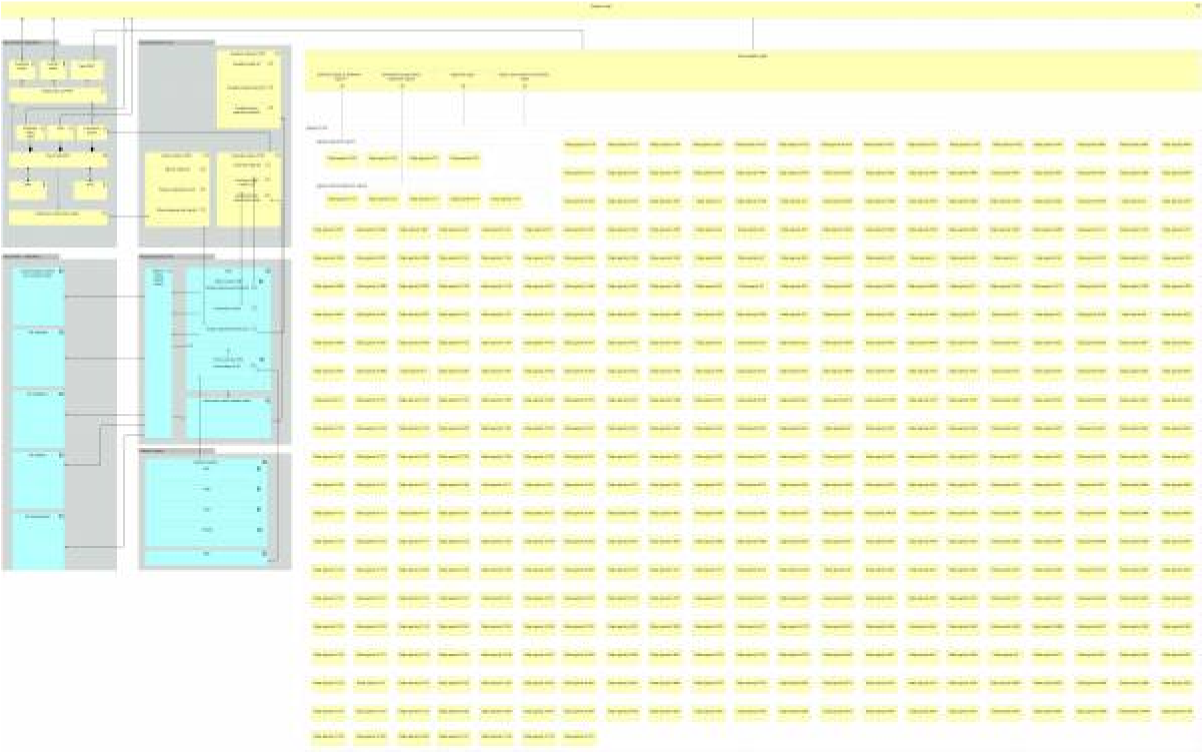
Figure 5: View of the future state of PPDF in terms of its components, services, actors, HW and SW technologies and physical interconnection



View of the business logic and data extraction of VS agendas

The following architectural diagram illustrates the future state of the PPDF from the perspective of a rights holder. A rights holder can access its data in the PPDF using specific interfaces provided by the PPDF reader. The aim is for the right holder to access all his data in all public administration agencies of the Czech Republic using the most convenient access for him.

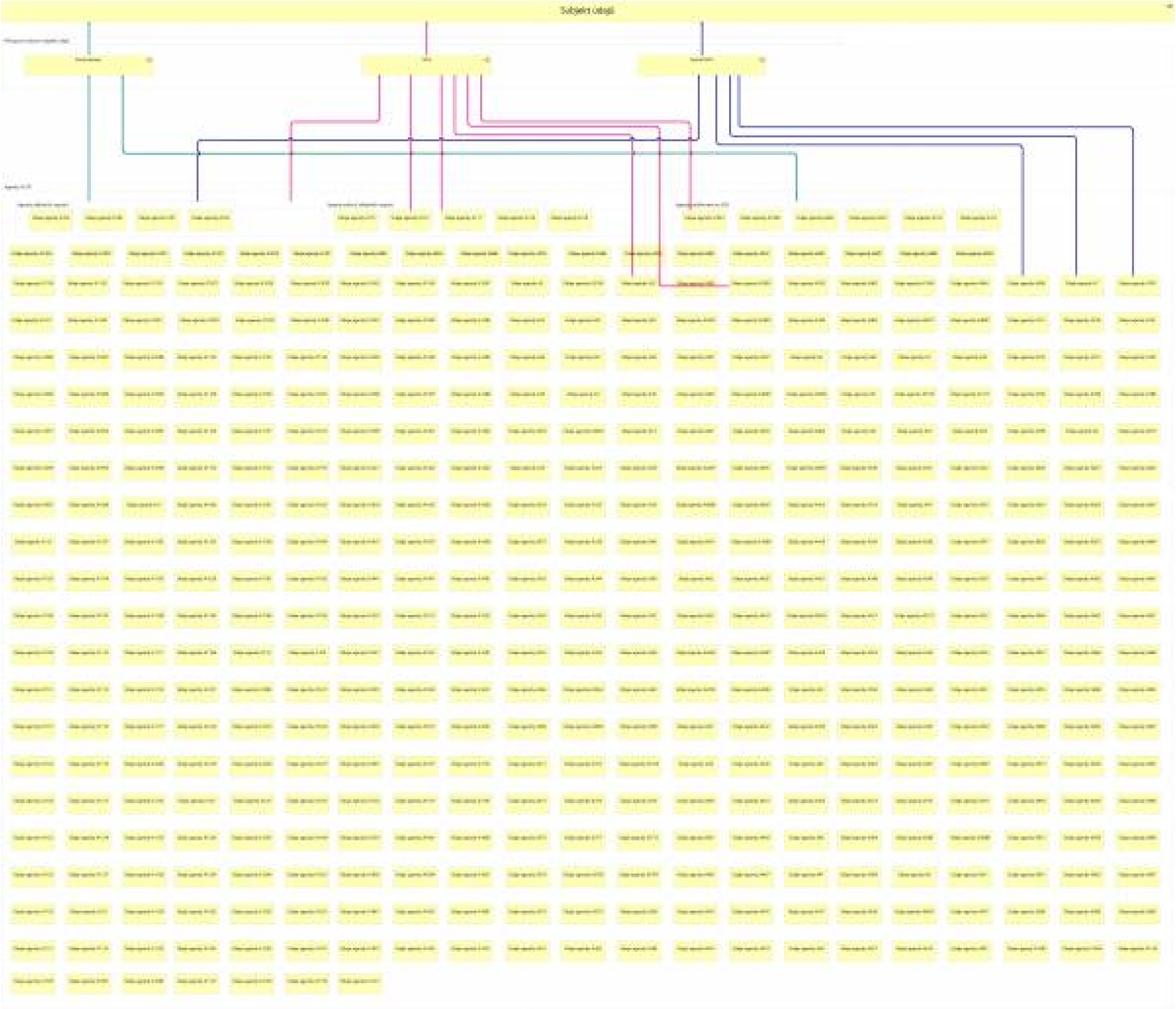
Figure 6: Viewing the future state of the PPDF from the perspective of the right holder



View of the business logic from the perspective of the rights holder

The following architectural diagram illustrates the current state of PPDF from the perspective of the rights holder and their ability to access the data of each agenda. The individual unbound agendas do not currently provide any data to the subject using PPDF services, yet they are shown here to show the breadth that PPDF is intended to encompass for the rights holder.

Figure 7: Viewing the current state of PPDF from the perspective of the rights holder



Relationship between PPDF and VDF

In addition to the PPDF, data is also shared through the Public Data Fund (PDF). Through the VDF, data is shared in the following scenarios:

1. When sharing data via the PPDF, the OVM needs the content of a codebook or the definition of selected codebook entries managed by another OVM. It does not receive them via PPDF but via VDF as open data.
2. The OVM does not perform an administrative activity but performs another complementary task (e.g. compiling an analytical report). It then uses public data in the form of open data available from the VDF. The difference with general open data and open data available from the VDF is that the data in the VDF is guaranteed to be available to the OVM and the publishing OVM guarantees its accuracy.

Other than through PPDF and VDF, no data is exchanged between OVMs.

From the perspective of PPDF, the first scenario is important. The second scenario is elaborated in more detail in the VDF Architecture document. The aim of the first scenario is to avoid duplication and uncontrolled and unconceptual extension of the codebooks in different ISVs. If an OMC needs a codebook managed by another OMC to interpret data obtained from the PPDF, then this OMC does not create a copy of the codebook in its information system in the form of a new codebook. In the data obtained from the PPDF, it obtains the IRI of the codebook entries that encode the data values. It obtains the full data of the codebook entries by dereferencing the IRIs in the VDF. There it also obtains the IRI of the codebook and by further dereferencing it can obtain the full codebook if necessary. However, if it stores the codebook, then it always does so only for optimization or availability reasons and always keeps this copy up-to-date with respect to the source via the VDF. The specific mechanisms are described in the VDF Architecture.

In the future, the set of data types that are not shared via PPDF but only exclusively via VDF may be extended from just dialers to other types.

Component Description

The Linked Data Facility (also referred to as PPDF) is a subject area consisting mainly of the Basic Registry Information System and the Shared Service Information System, whose services are published through the Central Service Point. The PPDF and its systems/services are the physical representation of the public administration reference interface. The basic function of the PPDF is to implement the principles of "Once-only" and "Data circulate, not people" into the common practice of public administration in the Czech Republic.

PPDF is the primary source of valid and legally binding data for the subjects of law and for all OVM and SPUU in the exercise of their competences. Thus, the PPDF will lead to the replacement of manual interactions between authorities by automated data exchange between different Agenda Information Systems.

The link between the Agency Information Systems and the basic registers is provided by the Basic Registers Information System, while the link between the Agency Information Systems and each other is provided by the Shared Services Information System.

All service provision within the PPDF is always linked to the basic registers by means of reference links to reference data on subjects of law (natural persons, legal persons and OVM) and reference data on objects of law (territorial elements and rights and obligations). For the reference links of data on natural persons, the Agency Identifier of Natural Persons (AIFO) is used, for the reference links of legal persons and natural persons in business, the Personal Identification Number (PIN) is used, and for the reference links of territorial elements, their respective identifiers assigned by RUIAN are used.

In addition to the development and support of the linked principles of data stem management and pseudonymisation, the main objective of the PPDF is the development of data sharing with additional agency sources of non-public data from key areas of public administration (transport, health, social services...) with a clearly defined guarantor and editor. There is a greater emphasis on interoperability between EU Member States, and the PPDF will be ready to provide services for cross-border data exchange, as described more in Chapter 4.

In realistic 2020, about 3,500 information systems out of a total of about 7,000 are connected to PPDF services. In addition to connecting all public administration information systems, the basic objective of the PPDF is to ensure that the connection for the relevant ISVS is not only reader-type (drawing data) but also publisher-type (providing their data). It is only when all relevant public administration information systems are drawing on and providing PPDF services that we can speak of a connected data pool.

The basic services of the PPDF for authorised PPDF readers are:

- Identification (assignment of an identifier) of the subject/object of the right held in the AIS and thus support pseudonymisation.
- Issue of data on the subject/rights holder according to the required context within the scope of the authorisations held in the RPP for the relevant AIS-supported agenda.
- V on changes to reference and agency data for data held in AIS.
- Support for claiming erroneous data.

Reference interface

The reference interface, in accordance with its de facto definition, means the interface for the implementation of links between public administration information systems, especially in the implementation of the interconnected data pool by sharing data between individual agency information systems in the form of shared services. The reference interface is therefore the communication interface for the provision and use of shared services by individual administrators of public administration information systems.

Access to the services of the reference interface is possible at the network level only through the Central Service Point (CMS), i.e. the Communication Infrastructure of Public Administration (CIPA), which is defined in Act 365/2000 Coll. The Central Service Point is a system whose primary purpose is to provide a controlled and registered connection of the information systems of the OVM and the SPUU to services (applications) provided by information systems of other entities with defined security and SLA parameters, i.e. access to eGovernment services. CMS can thus be called a private network for the performance of public administration on the territory of the state.

Connection to the CMS can be realized through:

1. Non-public KIVS operator (Regional Networks, Metropolitan Networks, ITS of the Ministry of Interior and others).
2. Public KIVS operator (KIVS operator competition through the central contracting authority of the Ministry of the Interior).
3. IPsec VPN.
4. SSL VPN.

Communication between individual OSSs is conducted exclusively via KIVS/CMS, i.e. individual OSSs are obliged to access public administration information systems only via KIVS/CMS.

The centrally managed and administered part of the reference interface ensures data sharing in the interconnected data pool with respect to Act 111/2009 Coll. on basic registers with central provision of all requirements imposed on the reference interface.

This centrally controlled and managed part of the Reference Interface consists of three components.

Table 1: Components of the centrally managed and administered part of the reference interface

Component	**Abbreviation**	**Description of functionality**
Basic registers information system	ISZR	
Information Sharing Service System	ISSS (formerly also eGSB)	Interface for sharing and exchanging data between ISVS and making links between them.
Information system for bulk data output in multiagenda queries (Form Agency Information System)	FAIS	It is used for processing queries and outputting data in the form of forms, including bulk forms, also from multiple PIs or other ISVS. Queries and outputs are transmitted via Data Boxes.

The use of data via the reference interface is always made exclusively on the basis of the relevant authorisations recorded in the RPP, but this does not mean that the RPP controls the actual release of data. The final decision whether or not to provide data is always the responsibility of the source AIS (the one whose data is requested). It makes this decision on the basis of the reference entitlement data recorded in the RPP.

In the future development of the PPDF, it is envisaged that authorisations for data or specific services will be checked by the ISZR and ISSS using reference data from the RPP. The end state should therefore be that the requesting system calling the service receives the requested data or information that it does not have the necessary permissions for the request. The permissions, and therefore the access to data and services, would therefore not have to be done by the system or its administrator, but everything would be managed using the RPP reference data.

Through the reference interface:

- The entry and editing of data in the basic registers is carried out.
  - The editing of the basic registers is carried out by the editors of the basic registers using the services of the external interface of the ISZR.
- Exploitation of data from the basic registers.
  - With regard to the permissions to access data in the basic registers, according to the announcement of the individual agencies in the RPP, using the services of the external interface of

    - the ISZR.
    - Notification of data changes and updates of basic registers data are also implemented using the services of the external interface of the ISZR.
- Data exchange in the form of shared services between AIS is implemented.

Implemented by OVM between each other using services and data exchange. In case of data exchange on natural persons, performs translation of AIFOs through ORG services.

- Implement bulk data output and query and response composition services for multiple data.
    - Implemented by the FAIS component and used by OVM or SPUU with appropriate authorization.
    - FAIS makes calls to the ISZR and ISSS services on the basis of a request received via the data box and returns the compiled response to the requester again via the data box.
- Implement the services of notification of data changes and data updates in individual agendas using the central component.

Basic rules for the use of the reference interface:

- Comply with the Decree on Act 365/2000 Coll. on Public Administration Information Systems, especially on the technical and functional parameters of the connection to the reference interface.
- The reference interface shall be accessed by the OVM through its AIS and by the SPUU through its PIS or through the AIS of another OVM.
- Each AIS or DMS of a PSC accessing the reference interface shall prove its identity by means of a system certificate issued by a Certification Authority under the management of the HRA.

- When exchanging data on subjects or objects of law, it is verified whether these subjects (ROB, ROS) or objects (RÚIAN, RPP) are listed in the basic registers (verification of the reference link).
- The OVM or SPUU requesting data on a specific subject is responsible for its proper identification in its agenda, i.e. obtaining the AIFO if it is a natural person or the ID number if it is a legal person or an entrepreneurial natural person. If the subject is not properly identified, then the data held in the AIS may be indicative only.
- Records (logs) of the identification of the requesting system, the time of response, the structure and content of the data provided shall be kept by the providing system. The identification of the providing system, the time of receipt of the response, the structure and content of the data shall be kept by the receiving system. The reference interface shall record the identification of both systems, the time and the structure of the data transmitted.
- Procedural interfacing with the filing service (eSSL) when the reference interface is used to transmit documents according to the rules of the filing service. This only applies to situations where the content is actually a document and therefore not just a data transfer.

Information system for the management of the use and publication of data of the reference interface of the public administration of the Czech Republic

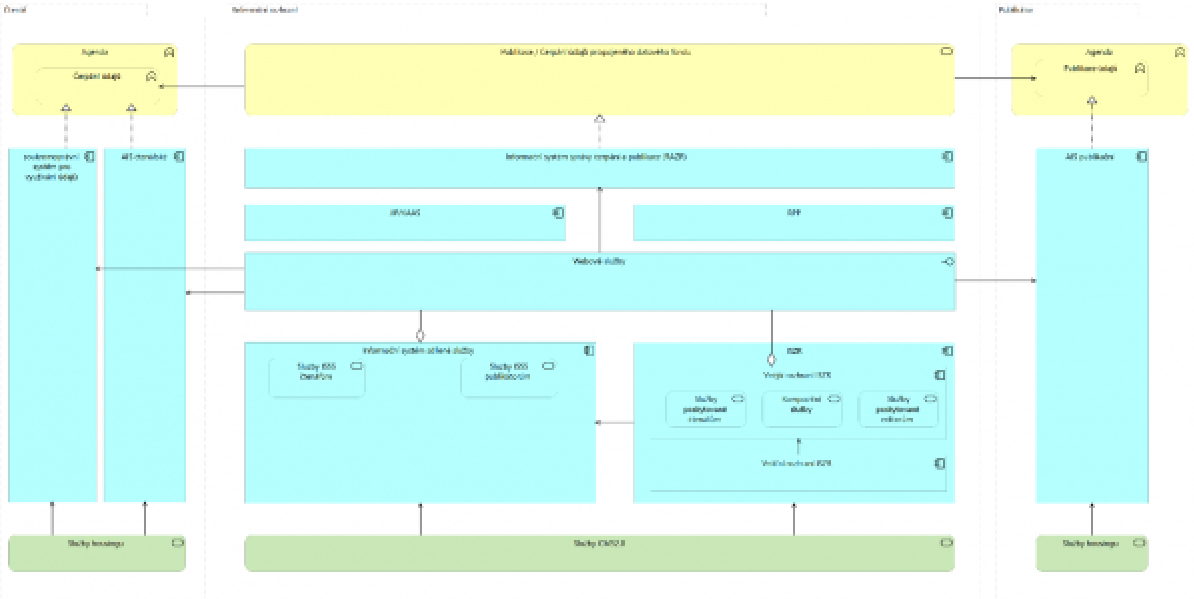
The Information System for the Management of the Extraction and Publication of the Data of the Public Administration Reference Interface of the Czech Republic (also referred to as the "Connection Management System") is a Public Administration Information System that allows any entity that is connected to the Public Administration Reference Interface (according to Act 365/2000 Coll. on Public Administration Information Systems) to manage data on information systems that provide or extract data through the Reference Interface.

The link management system will be created as an extension of the current RAZR system (registration authority of basic registers) or as a new system and must support the following functionalities:

- Login via JIP/KAAS
- Login via the NIA system
- Registration of all connected IS (agency information systems and private data use systems) according to the register of public administration information systems
- Records of all subject administrators of connected IS and their administrators (editors)

- Records of all contexts according to the agendas defined in the RPP
- Control of data permissions according to RPP
- History of the use and publication of data of the connected IS according to the logs of the reference interface
- Individualisation of information for logged-in and authorised user
- Enabling reporting of unauthorised use / provision of data, including monitoring of the progress of processing

- Enabling reporting of certificate misuse, including progress tracking
- Enable ordering of a new certificate, including progress tracking
- Enabling context management (creation, modification, deletion)



Reference interface design

Basic registry information system

The information system of basic registers is legislatively enshrined in Act No. 111/2009 Coll., on basic registers. The ISZR is a public administration information system, through which data sharing between the basic registers with each other, basic registers and agency information systems with each other, management of data access permissions and other activities is ensured. The ISZR consists of two basic interfaces.

Table 2: Interfaces of the ISZR

Interface	Main users	Description of functionality
Services of the internal interface	Only the ISZR in relation to the basic registers	
External Interface Services	Agenda Information Systems	

In particular, the following are implemented through the ISZR services:

- Access to data held in the basic registers.
- Services of complaint, contestation, notification of data changes, updating of data from basic registers.
- Entry and changes to data in the basic registers.
- Translation of agency identifiers of natural persons.
- Enforcement of compliance with the authorisations recorded in the RPP.

To connect to the basic registers, users follow the table below:

User	Path	Provides		
Subject of the right	Cannot access directly, indirectly e.g. through the citizen's portal or universal contact points and extracts from it.	Citizen's portal, public administration contact points or FAIS (sending a request via data box) through published forms. Data extraction and data complaints are ensured. The data obtained can be used in the forms of another OVM forms administrator.		
Authority of the public authority	With its Agenda Information System.	Provided by the Basic Registers Administration after fulfilling the conditions.		
		Agenda information system of another administrator.	Provided by the administrator of the AIS.	
	Through the CzechPOINT@office interface.	Provided by the Ministry of the Interior of the Czech Republic, the CzechPOINT@office administrator in cooperation with the local administrator.		
Private data user	Through the end-user information system built by the OVM.			
	Private legal information system for data exploitation.	Provided by the DPA authorised to operate such a system.		

In order to connect the agency information systems to the basic registers, certain basic conditions must be fulfilled, which are laid down by the Administration of the basic registers in its operational documentation for the ISZR. In particular:

1. The AIS administrator must have its IS registered in the ISVS register in the RPP
2. It must have declared in the RPP the competence in the agenda(s) it will perform with this AIS for the relevant OVM
3. The AIS administrator must indicate in the RPP which OVMs/SPMUs can access the RO or other AISs via its AIS.
4. The AIS must be connected to the relevant access point (KIVS or Internet). The method and process of connecting the AIS to the KIVS is outside the scope of the RoW system
5. The AIS must be certified to access the eGON interface. Certification is a process within the competence of the SZR. Within this process the scope of the AIS is defined - agenda, agenda roles and OVM This process is described in a separate document available on the SZR website.
6. The AIS must be issued with an electronic client certificate. The issuance of the client certificate is the last step in the AIS certification process, which is carried out by SZR
7. The AIS must be allowed access to specific eGON services within the RAZR (Registration Authority of the RoW) according to the security profile. Permissions to individual data are defined based on the OVM / agenda / agenda role combination, and are derived from the information in the RPP
8. Must have implemented calls to the eGIS services in its AIS, or be able to properly call, consume and use the web services of the eGIS external interface according to the eGIS operational documentation

Basic registries

The basic registers are a reference data source of data on subjects and objects of law and on the performance of public administration. These are reference data on

- natural persons,
- legal persons and natural persons engaged in business,
- addresses, territorial elements and real estate,
- public authorities and private data users,

- agendas and scope of public administration,
- certain decisions amending reference data.

The basic registers thus form the backbone of an interconnected public administration data pool, including a mechanism for pseudonymisation and linking of identifications from individual agencies. In addition, they provide, in particular, individuals with an overview of the use of their data by individual readers (OVM, SPUU, etc.) and the provision to others.

Reference data

Reference data are data held in the basic register which are marked as reference. It is a general legal and procedural premise that reference data are considered correct in the exercise of public administration unless proven otherwise or unless they are called into question by the relevant editor. It is therefore the case that the public administration must act on the basis of these reference data and, conversely, that if the public administration acts on the basis of these reference data, there can be no maladministration due to inconsistency with the facts.

Recording and editing of reference data

The editing and recording of reference data is always the responsibility of the relevant editor. The distinction between the editor's responsibility and that of the individual data is not a matter of the subject. There is also a situation where there is more than one editor per subject. In this case, the editors are divided into primary and secondary editors. The primary editor is responsible for the actual existence of the entire record (including creation, update and deletion), whereas the secondary editor is responsible only for the individual entity data (including updates). A typical example of a situation of a primary and a secondary editor are legal entities, where the relevant primary editor is responsible for the creation and registration of the relevant basic data (the court of registration, the regional office, the trade department of the municipality, etc.) and the secondary editor (the Ministry of the Interior as the ISDS administrator) is responsible for the additional data, e.g. on the data box. Therefore, the secondary editor cannot establish or cancel the entity, but only adds additional data to it.

The basic duties of the editor are therefore:

- To write and edit data on the basis of the procedural execution of the agenda, which determines whether there is a document registered in the filing service for the execution.
- To deal with the complaints process, including challenging the accuracy of the data from the base register manager, the editor himself or any public authority.
- Ensure the accuracy and timeliness of the data.

Virtual reference data

Virtual reference data are those data that are created by deriving, merging or otherwise modifying existing reference data. Thus, these data do not meet some of the requirements of traditional reference data, such as the responsibility of a specific editor. Virtual reference data have a label, a definition and a described process for how they are created in each specific service that can provide them. A typical example would be the virtual reference data "full name", which is composed of the reference data "first name or first names" and "last name". Other such virtual data may be:

- Age,
- name without accents,
- address in uppercase only,
- number of days until expiration of the identification document,
- telephone number in international format,
- etc.

Virtual reference data may not be explicitly mentioned in the law as content of a specific basic registry, as they are created and terminated with the call of a given ISZR or ISSS service, but are maintained in the RPP as a special type of data with a link to specific data of the basic registry.

At present, no ISZR or ISSS service has the possibility to provide virtual reference data. This functionality is foreseen in the framework of the development of the PPDF.

Indicator data type

An indicator is a reference data held in the basic register which serves to indicate that potentially relevant data on an entity are held in other information systems. The purpose of indicator data is to prevent unnecessary queries to information systems where such information is not held. The introduction of an indicator into the basic register is conditional on its inclusion as reference data in Act No 111/2009 Coll., on basic registers. In order to initiate such a legislative modification, it is necessary to assess whether the introduction of the new indicator will fulfil the purpose of eliminating unnecessary queries to the agency information systems (the indicated data occurs for a significant minority of persons or objects).

For a reference data of the indicator type, all the corresponding processes must be in place as for other reference data. Thus, a data editor must be identified, including the publication of services for editing the data by this editor, and other processes of the reference data life cycle must be ensured (complaints, notification of data changes, provision of data on request of the subject, etc.).

The administrator of the basic registry is responsible for the allowed set of indicators, including their names.

The editor of the indicator data type is the information system administrator, who maintains the indicated data and enters them into the basic register in the same way as the reference data, i.e. by automatic processes. An indicator may also be a virtual data of the basic register and multiple indicators may relate to one subject.

The indicator data type has the following basic attributes:

- name - the unique name of the indicator,
- AIS identifier + agenda identifier,
- optional identifier of the context within which detailed data can be retrieved via ISSS,
- optional refinement code,
- optional text refinement.

The indicator data type contains other standard attributes:

- validity start date and time,
- expiry date and time,
- date and time of initial entry,
- date and time of last change,
- status (S, N, X, F).

Currently no ISZR or ISSS service has the capability to provide an indicator. This functionality is foreseen in the development of the PPDF, where the following modifications are required to implement this data:

- Add to AuthorizationInfo a text item ListIndicator, a string type, and structures for writing and reading. The names of the flags to be returned/written are entered into the ListIndicator. It is the equivalent of a ListIndicator, and the ISZR checks that the querying AIS has permission to read or write to a particular indicator.
- Access to indicator type data is controlled in the standard way by the Rights and Obligations Register. A user (OVM, agenda, activity role) must be allowed to access an indicator with a given name.

Data accuracy complaint process

Anyone who has doubts about the correctness of a reference can initiate the process of claiming the correctness of the reference. The process itself is then always handled by the primary source of the data - i.e. its editor. The process starts with the receipt of a message containing a doubt about the correctness of the data (from another OVM, a right holder, a registry administrator, etc.). The editor is then obliged to mark the data in question as questionable. Subsequently, the editor of the data must perform a validation of its correctness, which may result in the closure of the complaint as unjustified (and thus preserving the value of the data) or justified (and thus changing it to the correct value). At the same time as closing the claim, it removes the doubt from the data. The claim process itself is governed by the Administrative Procedure Code.

Use of reference data

Each public authority is obliged to use reference data from the basic registers within the scope of its competence in the individual agencies. In doing so, it either uses the services and links to its agency information systems or uses one of the other tools.

The basic obligations of the OVM and the SPÚÚ using the data are therefore:

- To use reference data in the agendas.
- Use up-to-date reference data, which can be achieved in one of two ways or a combination of the two, but always in accordance with the operational documentation of the ISZR:
    1. Using the mechanism of notification of changes to reference data and subsequent updates, or
    2. by querying the base registers for each transaction.
- If a discrepancy between the reference data and the reality is detected, implement a data complaint against the data editor.
- Do not request the data held in the registers from the right holder.

Registry of Population (ROB)

The Population Register is a basic register according to Act No. 111/2009 Coll., on basic registers[1)], which records reference data on natural persons. The administrator of the Population Register is the Ministry of the Interior. The primary editors are the Ministry of the Interior and the Police of the Czech Republic through the Agenda Information System for Population Registration and the Agenda Information System for Foreigners. The subjects of the rights recorded in the Population Register are:

- citizens of the Czech Republic,
- foreigners residing in the territory of the Czech Republic under permanent residence or on the basis of a long-term visa or long-term residence permit,
- citizens of other Member States of the European Union, citizens of States bound by an international treaty negotiated with the European Community, citizens of States bound by the Treaty on the European Economic Area and their family members who reside on the territory of the Czech Republic as part of their permanent residence or who have been issued a document of temporary residence on the territory of the Czech Republic for more than 3 months,
- foreigners who have been granted international protection in the form of asylum or subsidiary protection in the Czech Republic,
- other natural persons for whom another legal regulation requires an agency identifier of a natural person and stipulates that these natural persons shall be entered in the population register.

The reference data on natural persons are:

- surname, maiden name,
- first name, where appropriate,
- gender,
- the address of the place of residence, or, where applicable, the address to which documents are to be served in accordance with another legal regulation; these addresses are recorded in the form of a reference link (address location code) to the address reference in the territorial identification register; in the case of an address to which documents are to be served pursuant to another legal regulation, the identification of a post box or a delivery box or an address which is outside the territory of the Czech Republic and which has not been assigned an address place code in the territorial identification register is also recorded; in the case of an address of a place of residence, this information is marked as the address of the office if it is marked in the same way in the information system of the population register or the information system of foreigners,

- the date, place and district of birth, in the case of a subject of law who was born abroad, the date, place and state where he was born; the information on the place and district of birth on the territory of the Czech Republic is kept in the form of a reference link (territorial element code) to the reference in the territorial identification register,
- the date, place and district of death, if the death of the subject of the right is outside the territory of the Czech Republic, the date of death, the place and the State in whose territory the death occurred; if a court decision is issued declaring the subject of the right to be dead, the date indicated in the decision as the date of death, or as the date on which he/she did not survive, and the date on which the decision became final shall be entered; the place and district of death in the territory of the Czech Republic shall be entered in the form of a reference link (territorial element code) to the reference entry in the territorial identification register,
- nationality, or multiple nationalities, if applicable,
- limitation of legal capacity,
- marital status or registered partnership,
- numbers and types of identification documents and their expiry date,
- the type of data box and the identifier of the data box, if this data box is accessible.

Non-reference data on natural persons are also recorded in the population register:

- a telephone number for the public mobile telephone network or an e-mail address for sending a selected range of information,
- serial number, issuer and validity of the qualified certificate for electronic signature,
- personal security code, which is authentication data for the purposes of the population register (it is kept in encrypted form and is not public),
- the agenda identifier of the natural person, which is the identifier for the population register agenda.

The population register also holds operational data

- a record of the use of data from the population register for the purposes of agency information systems,
- a record of the disclosure of data to the subject of the right or to another person, which includes the date and time of the disclosure, an identifier of the consent of the subject of the right to disclose the data to another natural or legal person and the identification of the person who disclosed the data,
- the date of the last change to each entry in the population register,
- a record of the granting or withdrawal of the right holder's consent to disclose the data to another natural or legal person.

The data editors are:

- in the case of citizens of the Czech Republic, the editor is the Ministry of the Interior, which records the data through the agency information system of the population register and the register of identity cards or the register of travel documents,
- in the case of foreigners, the editor is the Police of the Czech Republic or the Ministry of the Interior, which record data through the agency information system on foreigners,
- for data boxes, the Ministry of the Interior as the administrator of the Data Box Information System is the editor,
- for non-reference data, the Ministry of the Interior and the Administration of Basic Registers are the editors.

Register of Persons (ROS)

The Register of Persons is a basic register according to Act No. 111/2009 Coll., on basic registers, which records reference data. The administrator of the register of persons is the Czech Statistical Office. The primary editors are authorities and institutions that are already legally obliged to register persons. These include the Commercial Register, the Trade Register, registers or information systems of selected ministries and central government bodies, professional chambers, municipalities, regions, etc. The Ministry of the Interior with the Data Box System (ISDS) and the Ministry of Justice with the Insolvency Register are secondary editors.

The subjects of law maintained in the register of persons are:

- legal entity,
- organizational unit and organizational unit of a legal person,
- organisational unit of the state,
- an internal organizational unit of an organizational unit of the state, if this internal organizational unit is entrusted by law with its own competence,
- an entrepreneurial natural person,
- a foreign person and an organisational unit of a foreign person,
- trust fund,

if they are entered in the register pursuant to this Act or another legal regulation.

The reference data on legal persons are:

- business name or designation or name, if applicable, and surname, if the natural person engaged in business is not registered in the Commercial Register,
- the name or, where applicable, the first and last names of the natural person engaged in business or of the foreign person and the organisational unit of the foreign person; if the person is entered in the population register, this information shall be kept in the form of a reference link (agency identifier of the natural person) to the reference entry in the population register,
- the agenda identifier of the natural person for the agenda of the register of persons,
- person identification number,
- date of creation or date of registration under other legislation,
- date of termination or date of deletion from the register under other legislation,
- legal form,
- type of data box and identifier of the data box, if this data box is accessible,
- the statutory body, expressed by reference to the population register or the register of persons or by the name, surname and residence of a natural person or the name and registered office of a legal person, if these persons are not entered in the population register or the register of persons,
- a liquidator expressed by reference to the population register or the register of persons, or by reference to the name, surname and residence of a natural person, if applicable, or to the name and registered office of a legal person, if these persons are not entered in the population register or the register of persons,
- the guardian of a legal person, expressed by reference to the population register or the register of persons, or by reference to the name, surname and residence of a natural person, if applicable, or to the name and registered office of a legal person, if these persons are not entered in the population register or the register of persons,
- the insolvency administrator, expressed by reference to the population register or the register of persons, or the name, surname and residence of a natural person or the name and registered office of a legal person, where these persons are not entered in the population register or the register of persons,
- a receiver expressed by reference to the population register or by the name, surname and residence, where applicable, of the person concerned, if that person is not entered in the population register,
- legal status,
- the address of the person's registered office; if the building is a building recorded in the territorial identification register, this information shall be recorded in the form of a reference link (address location code) to the address reference in the territorial identification register,
- date of commencement of the activity at the establishment,
- the identification number of the establishment,
- the date of cessation of the activity at the establishment,
- the address of the place of establishment; where the building is a building recorded in the territorial identification register, this information shall be entered in the form of a reference link (address place code) to the address reference in the territorial identification register,
- the address of the place of residence in the Czech Republic in the form of a reference link (address place code) to the address reference in the register of territorial identification, or the residence abroad of the natural person referred to in § 25(e) and (f); in the case of persons entered in the register of residents,

the address of the place of residence in the form of a reference link (agency identifier code of the natural person) to the reference of the natural person in the register of residents,
- interruption or suspension of activities under another legal provision; in the case of activities corresponding to one agenda, the interruption of all such activities.

Non-reference data on legal persons shall also be kept in the register of persons:

- a telephone number for the public mobile telephone network or an e-mail address for sending a selected range of information.

Operational data shall also be kept in the register of persons:

- agenda code,
- editor's personal identification number,
- date of initial entry in the register of persons,
- date of the last change to the data recorded in the register of persons,
- record of the use of the data from the register of persons.

The current list of data editors in ROS is published on the following website: https://www.czso.cz/csu/czso/editori-ros. For non-reference data, the editor will be the Ministry of the Interior.

Name of the person	**Type of person**	**ROS editor**
Attorneys	FO	Czech Bar Association
Employment Agencies	FO	Ministry of Labour and Social Affairs
Accredited person under the Consumer Credit Act	FO	Czech National Bank
Auditors	FO	Chamber of Auditors of the Czech Republic
Road Safety Auditors	FO	Ministry of Transport
Authorized Architects	FO	Czech Chamber of Architects
Authorized Engineers and Technicians	FO	Czech Chamber of Authorized Engineers and Technicians Active in Construction
Churches and Religious Societies	PO	Ministry of Culture
Czech National Bank, Czech Television, Czech Radio, Regional Council of the Cohesion Region, General Health Insurance Company	PO	Ministry of the Interior
Tax advisors	FO	Chamber of Tax Advisors of the Czech Republic
Voluntary associations of municipalities	PO	Locally competent regional authority or the Municipality of the capital city Prague
License holders for business in energy sectors	FO	Energy Regulatory Office
European Groupings for Territorial Cooperation	PO	Ministry for Regional Development
Natural Persons - Operators of Postal Services	FO	Czech Telecommunications Office
Persons operating a trade (tradesmen)	FO	Locally Competent Trade Licensing Authority
Community associations	PO	Locally competent municipality with extended competence, Ministry of Agriculture
Insolvency administrators	FO	Ministry of Justice
Investment intermediaries	FO	Czech National Bank
Communal Contributory Organisations	PO	Counties, Municipalities
Mediators	FO	Ministry of Justice
International military organisations established on the basis of an international treaty	PO	Ministry of Defence
Foundations and endowments	PO	Registrar's court with local jurisdiction
FO	FO	Chamber of Commerce of the Czech Republic
Public benefit corporations	PO	locally competent court of registration

Name of the person	Type of person	ROS editor
Commercial companies; cooperatives, business units, other persons registered in the Commercial Register	PO	Locally competent court of registration
Trade unions and employers' organizations, affiliated trade unions and employers' organizations, international trade unions, international employers' organizations, affiliated international trade unions, affiliated international employers' organizations	PO	Locally competent court of registration
Organizational units of the State	PO	Ministry of the Interior
Persons handling high-risk biological agents and toxins	FO	State Office for Nuclear Safety
Persons carrying out mining and mining-related activities	FO	Czech Mining Authority
Persons involved in the production and distribution of pharmaceuticals	FO	State Institute for Drug Control
Persons authorised for exchange and foreign exchange activities	FO	Czech National Bank
Persons using nuclear energy and ionizing radiation	FO	State Office for Nuclear Safety
Patent Attorneys	FO	Chamber of Patent Attorneys of the Czech Republic
Entrepreneurs in electronic communications	FO	Czech Telecommunications Office
Insurance intermediaries	FO	Czech National Bank
Political Parties and Political Movements	PO	Ministry of the Interior
Audiovisual Media Service Providers	FO	Radio and Television Broadcasting Council
Providers of small-scale payment services	FO	Czech National Bank
Healthcare service providers	FO	Locally competent regional authority or the Capital City Municipality Prague
Providers of social services	FO	Locally competent regional authority or the Municipality of the Capital City of Prague Prague
Operators of aerial work and airport operators	FO	Civil Aviation Authority
Operators of professional veterinary activities	FO	State Veterinary Administration
Radio and Television Broadcasting Operators	FO	Radio and Television Broadcasting Council
Operators of emission measurement stations	FO	Local municipality with extended competence
Operators of technical inspection stations	FO	Locally competent regional authority or the Capital City Council Prague
Zoo operators	FO	Ministry of the Environment
Restaurate	FO	Ministry of Culture
Federal Insurance Claims Adjusters	FO	Czech National Bank
Federal Consumer Credit Intermediary	FO	Czech National Bank
Court Executors	FO	Executors' Chamber of the Czech Republic
Court Experts and Interpreters	FO	County Courts, City Court Prague
MO	PO	Registrar's Court with local jurisdiction
Clubs (formerly civic associations), affiliated associations (formerly an organizational unit of a civic association)	PO	Locally competent registry court
State Funds	PO	Ministry of the Interior
State contributory organisations	PO	Ministries and other central administrative authorities
Trust Funds	PO	Locally competent court of registration
School legal entities	PO	Ministry of Education, Youth and Sports
Institute	PO	Local registration court

Name of the person	**Type of person**	**ROS editor**
Bound representative according to the Consumer Credit Act	FO	Czech National Bank
Public and State Universities	PO	Ministry of the Interior
Public Research Institutions	PO	Ministry of Education, Youth and Sports
Public corporations - region, municipality, capital city of Prague	PO	Ministry of the Interior
Veterinarians authorised to carry out veterinary therapeutic and preventive activities	FO	Chamber of Veterinary Surgeons of the Czech Republic
Foreign legal entity, branch plant of a foreign legal entity, branch plant of a foreign natural person	PO	Locally competent registration court
Foreign association, foreign branch association	PO	Locally competent court of registration
PO	PO	Locally competent court of registration
Representation of a foreign bank	PO	Czech National Bank
Agricultural Entrepreneurs	FO	Ministry of Agriculture
Bonded consumer credit intermediary	FO	Czech National Bank
Special organization for representation of Czech interests in international NGOs, organizational unit of special organization for representation of Czech interests in international NGOs, international NGO, organizational unit of international NGO	PO	Locally competent court of registration

Register of Territorial Identification of Addresses and Real Estate (RÚIAN)

The Register of Territorial Identification of Addresses and Real Estate is a basic register according to Act No. 111/2009 Coll., on basic registers, which records basic territorial elements and addresses. The administrator of the Register of Territorial Identification is the Czech Geodetic and Cadastral Office. The primary editors are cadastral offices, through the cadastre information system, building authorities through the territorial identification information system, municipalities and the Czech Statistical Office.

The Register of Territorial Identification contains data on the following basic territorial elements:

- the territory of the state,
- the territory of a cohesion region according to another legal regulation,
- the territory of a higher territorial self-government unit,
- the territory of a region,
- the territory of a district,
- administrative district of a municipality with extended competence,
- the administrative district of a municipality with a designated municipal authority,
- territory of a municipality,
- the territory of a military district,
- administrative district in the capital city of Prague,
- the territory of a municipal district in the capital city of Prague,
- the territory of an urban district in the capital city of Prague,
- the territory of an urban district and an urban part of a zoned statutory city,
- cadastral territory,
- the territory of a basic settlement unit,
- building object,
- address place,
- land in the form of a parcel.

The register of territorial identification shall also contain data on special purpose territorial elements by means of which the territory is expressed by another legal regulation, if another legal regulation provides that such data shall be entered in the register of territorial identification and if these special purpose territorial elements are entirely composed of at least some of the basic territorial elements.

The territorial identification register shall also contain data on the following territorial registration units

- part of a municipality,
- a street or other public space .

The reference data in the territorial identification register are:

- identification data,
- data on links to other territorial elements or territorial registration units,
- data on the type and use of the land and its technical and economic attributes,
- data on the type and use of the building object,
- data on the type and method of protection of the property,
- addresses,
- locational data of cadastral areas and superior elements,
- locational data of territorial elements and territorial registration units - only in those cadastral territories where the cadastral map is kept in digital form.

Register of rights and obligations (RPP)

The Register of Rights and Obligations is administered by the Ministry of the Interior and information for controlling access to the data of other basic registers; at the same time, this register provides a basic overview of the agendas carried out by public authorities; information on citizens and legal entities is kept in this register on decisions that have led to changes in the data in the basic registers. Furthermore, the RPP serves as a source of information for the RoW information system in managing user access to data in the individual registers and agency information systems. This means that whenever a given subject attempts to obtain a certain data or even to change (edit) it, the system assesses whether the subject will be allowed to work with the data provided by the public administration on the basis of the legal authorisation, and thus the RPP becomes an important component of the RoW within the concept of using the interconnected data pool and sharing data across not only the state administration for the management of public administration performance.

The RPP includes in particular:

- public administration agendas and their responsibilities,
- list of Public Authorities and private users of data from the basic registers,
- a map of the competences of public authorities within the agenda model,
- data on data held in the agendas and on their provision and use,
- data on the entitlements of public authorities and private users to access data from the basic registers and agency information systems,
- decisions on the basis of which reference data in the Population Register and the Register of Persons are changed,
- a list of public administration information systems and their link to the agendas and data held in them.

The RPP also includes the technical structure of data, which, in addition to the obligations set out in the Decree on the Basic Registers Act 111/2009 Coll., is described in Chapter 3.2.

- Directory: a link to a dataset representing a codebook published in the National Catalogue of Open Data according to the rules of the Public Data Fund. If the data is created in the agenda, it is a reference that says the data is the source of the codebook, if it is a downloaded data, it is a reference to a codebook published by another entity.

The administrator of the Register of Rights and Obligations is the Ministry of the Interior, the primary editors are the notifiers of public administration agendas.

The basic elements for the agenda model of public administration are maintained in the RPP. There is also a map of the shareable data of individual agencies and technical data on the data held within individual agencies and permissions to access the data.

Another part of the RPP is the registration of public administration information systems, their link to the OVM, agendas, data on their administrators, etc.

Key roles in relation to basic registers

The following roles are defined in relation to the use of basic registers.

Table 3: Roles defined in relation to the use of the RoR

Roles	Description and meaning	Examples
Basic register manager	The public authority that manages the relevant basic register.	For ROB and RPP it is the Ministry of Interior, for ROS it is the CSU, for RÚIAN it is the ČÚZK.
Reference data editor	The public authority which, by law, edits and records reference data and is therefore responsible for their accuracy and is obliged to deal with complaints and data updates.	For ROB it is the Ministry of the Interior (e.g. through registration offices and registry offices), for ROS and RÚIAN it is the individual agency points according to the relevant laws.
Reference data user (reader)	A public authority or private user who is obliged or authorised to use reference data and accesses the RO for this purpose.	
Subject of the law	Specific natural or legal person about whom data are kept in the registers.	Each natural or legal person for its data. A legal person is always linked to a natural person.
Reporter of an agenda	Reporter of an agenda held in the RPP (cf. Agenda model of public administration).	For the registry agenda the Ministry of the Interior, for the health services agenda the Ministry of Health, for the pensions agenda the Ministry of Social Affairs
Authority acting in the agenda	Authority of public authority or SPUU which by law exercises competence in the agenda (see. Agenda model of public administration).	

Editorial AIS with composite services

Systems whose data is published by composite services. Composite services are defined as AIS services that provide data held in editorial AIS systems with a link to reference data held in the AIS:

- Population registry - AISEO (administered by the Ministry of the Interior of the Czech Republic),
- Foreigners Information System - AISC (Administered by the Police of the Czech Republic),
- Travel documents register - AISECD (Administered by the Ministry of the Interior of the Czech Republic),
- Registration of identity cards - AISEOP (Administered by the Ministry of the Interior of the Czech Republic),
- Information System of the Cadastre of Real Estate - ISKN (Administered by the Czech Office of Surveying and Cadastre),
- Information System of Territorial Identification - ISÚI (Administered by the Czech Geodetic and Cadastral Office),
- AIS Competence - AISP (Administrator is the Ministry of the Interior of the Czech Republic),
- eIdentity - not currently an editor of the basic registers, but provides data in relation to the reference record in ROB (administrator is the Administration of Basic Registers).

Each ROB has its own editors who edit the data. The editors enter data into the individual ROBs and together with the subject administrator of each of the editors, this keeps the data in the ROB correct and up-to-date. A data reclaim mechanism is used to ensure that the data is up-to-date and correct. Editors edit the data in the RoW using their editing information systems on the basis of the procedural performance of the agenda, which determines whether there is an obligation for the performance to have documents recorded in the eSSL or separate document filing systems in accordance with the legislation. The reader may draw non-referential data in the form of composite services. Since only the current data which are correct and guaranteed by the State are contained in the CR (except for the non-referential data contained in the basic registers), it is possible to retrieve other non-referential data (historical data on the subject of the law and other data not contained in the CR) from the editors' editing systems as part of the composite services.

Shared service information system

The Shared Service Information System (referred to in the IT environment as the eGovernment On-Line Service Bus, eGSB) is a unified interface for sharing data between agency information systems. It is part of the reference interface allowing individual OVM AIS to draw on and publish data held on individual legal entities. Where an agency is required by law to maintain its own data records, it is obliged to publish its data to other agencies through the ISSS as a secure, standardised and documented interface for authorised readers. It is managed and operated by the Basic Registers Administration and enables:

- Publish data sharing services for data relating to specific subjects and data objects.
- Use data sharing based on published services.
- Translation of agency identifiers of individuals for whom data is exchanged between agencies (AIFO translation).
- Exchange data files with data on subjects based on pseudonymised identifiers in relation to translated AIFO identifiers.
- Provision of complaint services, notification of data changes and updating of data provided by AIS services.
- Providing independent auditing of data exchanges (stores information identifying the query and response and the technical cryptographic fingerprint of the message - hash).

The aim is to ensure that public administration clients are not forced to provide evidence of facts that the public administration already knows about or that have even arisen from a public administration decision. Most of the facts needed for public administration decision-making are already recorded somewhere, in the form of data in public administration information systems. There are also facts which, although they are the basis for public administration decisions, are not yet recorded as data in the AIS (examples are study certificates, sheltered workshop agreements, etc.). The mapping of the data in the individual agencies, which is now taking place as part of the new reporting obligations of the notifiers to the RPP, has gradually established a basic map of the data recorded, required and provided in the individual agencies and where and how they are recorded and in which AIS. This, as already described above, creates a basic data map of the public administration and it is therefore possible to analyse it and identify those data and facts that are used in multiple agencies.

The functionality of the principle is verified on the reference data held in the basic registers, where the client does not have to prove these data and their changes, but the whole public administration obtains these data through services and then makes decisions based on them. The principle of data sharing through the ISSS is only an extension of this functional unit to include other data. Two main roles are defined for the use of ISSS.

Table 4: Roles defined in relation to the use of ISSS

Role	Description	What it does
The publisher (provider)	The ISVS administrator from which the data is provided.	Services publishing data through the ISSS, based on the agenda providing data from the AIS.
Reader (user)	OVM retrieving data from another agenda on the basis of its permission in RPP.	Connection to ISSS and calling publisher services (also multiple ISVS of a given agenda), AIFO translation from the provider's agenda is used, the reader calls according to the AIFO of its agenda in case of a natural person. No translation is used for a legal person.

In the context of data sharing via ISSS, the following aspects apply:

- The data is reported in the register of rights and obligations as data that the agenda processes on the

basis of legal authorisation.
- The data must be held in the AIS.
- It is clear for the data how it was created, who is responsible for its entry, changes, management and how it can be changed or cancelled.
- The data provider is always the AIS administrator in which the data is held and recorded.
- The data is always linked to the subject or object of the right in the RoW.
- It will be possible for the right holder to extract the data as an extract from the public administration information system.

As the aim is to link data efficiently and effectively, primarily to reduce the need for the client to prove facts, the data will be able to be retrieved by the public authority:

1. on the basis of the consent of the right holder (on behalf of the right holder), or
2. on the basis of a legal authorisation to keep the data in the agenda with the indication of the drawdown in the RPP (ex officio).

Context used in ISSS

Each agenda is defined by the relevant legislation. Within the agenda, the data necessary and specific for its execution are kept on subjects and objects. These data can also only be recorded on the basis of the relevant legal provisions. Subjects and objects are dealt with within an agenda in a certain context (given by the legislation), i.e. subjects and objects are understood in a certain 'context' within the performance of that agenda.

These contexts differ in the execution of different agendas, which is reflected, inter alia, by the fact that different objects are dealt with in relation to subjects in different agendas and different data are recorded and, where appropriate, exchanged on subjects and objects. We can therefore say that the context:

- determines the legal status of the entity (subject or object) within the agendas and
- the specific data (attributes) of the entity defined in the agenda are associated with it.

Methodologies for creating contexts address the detailed process

- Context Creation Methodology.
- Methodology for implementing a new context for an entity or data object passed through ISSS.

The context creation methodology introduces two levels of context - technical and conceptual. The technical level of context consists of an XSD schema that defines the syntax of the XML messages in which the shared data is expressed. In order to use ISSS services for a linked data pool, it is necessary to know in particular:

```
<ul>
```

```
<li>
```

>

```
<p>
```

Agenda from which the reader wants to use the data.

```
</p>
```

```
</li>
```

```
</ul>
```

```
<ul>
```

```
<li>
```

>

```
<p>
```

The agency that the reader is performing and in which the data is being read.

```
</p>
```

```
</li>
```

```
<li>
```

>

```
<p>
```

Context for querying data from the publishing AIS.

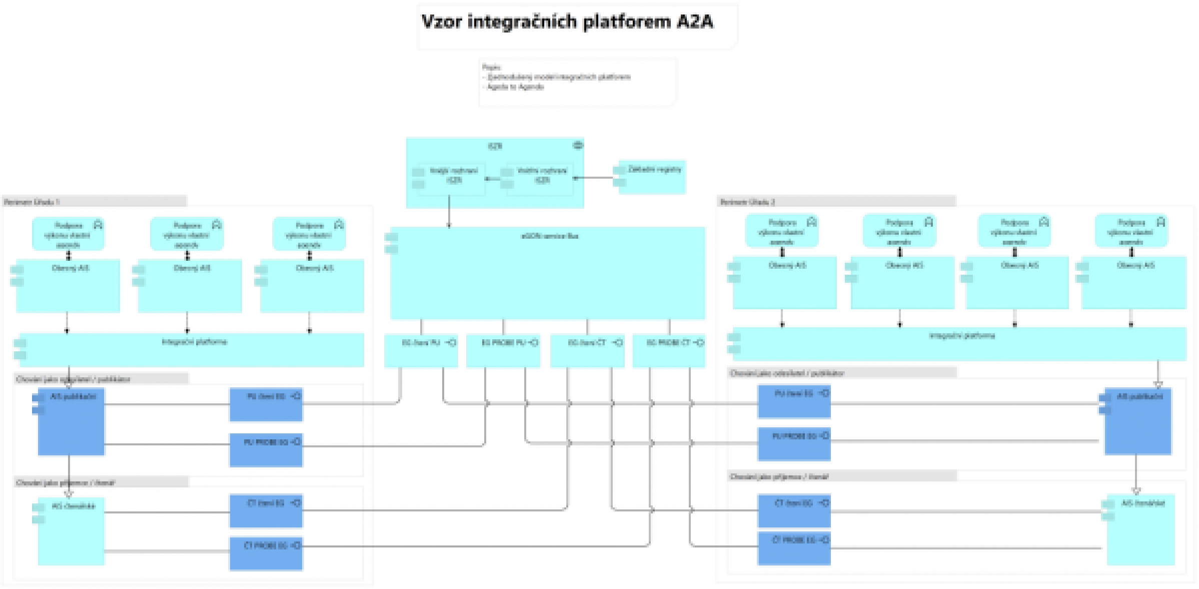
```
</p>
```

```
</li>
```

</HTML></ul></HTML>

Before using ISSS, the reader must first determine the context and its XSD schema, which will be used to receive query responses in ISSS. Therefore, he must first call a special ISSS service to read the Context Catalog, in which he then finds out which context he must call to get the data from the providing agency.

Figure 9: View of the integration platform interfaces



IS interface for batch data exchange

The Form-based AIS (FAIS) is a component of the ISZR which, through special form-oriented services, allows to request the release of multiple data from the basic registers and subsequently facilitates the batch release of these bulk data through the data mailbox. It is used for cases where it is mandated by law that reference data are used in multi-subject groups. This is the case, for example, for the issue of electoral rolls.

The FAIS is used to process the issue of data from the basic registers in the form of form requests to the data box of the ERO and responses to the data box of the applicant. For example, requests for data extracts, data usage reports, etc. are processed in this way. FAIS has an interface to the filing service according to the National Standard for Electronic Filing Systems. FAIS therefore provides, among other things:

- Voter lists provided to municipal election authorities.
- Dispatch of bulk batches of data according to the permissions in the relevant agenda.
- Execution of the right holder's request for extract of data from the systems connected to the reference interface, i.e. the entire PPDF.
- Compiling a summary of the data usage statement sent to the data box of the right holder.

FAIS operates according to the following points:

1. A data release request is compiled by the applicant and sent as a form to the CAP data box.
2. FAIS as a component of the ISZR retrieves the data message with the request form and processes the request, verifying the data authorisation and the release of the individual data.
3. After using the services of the ISZR and ISSS, FAIS compiles the response and sends it back to the applicant's data box in the given format.

FAIS is not primarily intended for use by agency information systems, but to process form requests authenticated by the identity of the sender of the request via his/her data box. For the use of the output of data from the basic registers, the external interface services of the ISZR are used by the agency information systems.

FAIS will provide the corresponding data extraction process via data boxes for all data published on the PPDF.

Entity records

The linked data pool is based on the exchange of data on uniquely identifiable subjects and objects. When recording, managing and linking data, it is essential to use the designated identifiers correctly and not to misuse identifiers already recorded.

An essential service that is part of the development of the linked data pool services is the service that returns the AIFO (agency identifier of an individual) for the current and historical document number and type. This service is necessary to replace persistent and meaningful identifiers such as the Birth Number as an identifier of a natural person not only in public administration processes and documents, but also in the private sphere.

Identifiers of subjects - natural persons

Within the framework of the linked data pool, a set of binding architectural recommendations for data exchange and data pool management (data registration) is established. This of course also applies to natural persons. In order to make the other parts of this document understandable, below is a table with a summary of the identifiers related to the natural person:

Name	Description	Examples	Serving for
Agenda Identifier of a Natural Person (AIFO)	An identifier that is assigned by ORG for a given agenda and is unique for the person and the agenda.	AIFO in the Population Registration Agenda, AIFO in the Driving Licence Agenda	Technical identifier for the purpose of uniquely identifying a natural person in an agenda and as a person identifier in data exchange. It is only in the agenda, it is never provided or transmitted, it is only translated via ORG.
Pseudonym from NIA (BSI)	Identifier assigned by NIA for each qualified service provider.	BSI for citizen portal, BSI for CSSA portal, BSI for general teaching hospital	
Style Identifier (SI)	Unique identifier originating from a public document that can be used to identify a person when communicating with a public administration. Any liaison identifier must be in the ROB, except for the BSI.	Document type and number (OP, passport)	Used in face-to-face or paper or electronic communication with the client, instead of or in addition to the CI. It is used to translate the KI for internal work in the agenda and AIS, and the AIFO in the agenda for communication within the PPDF. The AIS then knows both the AIFO and the KI, this identifier (SI) is not recorded or stored in the systems.
Client Identifier (CI)	Client number used in a given agenda or group of agendas of one OSC, as a meaningless identifier known to both officials and clients.	IDN, Insurance Number, Client Number	

Evidence of other natural persons

In the performance of public administration, a situation arises where the services provided do not concern a subject who is recorded in the basic population register. An example may be the purchase of real estate by a foreigner who has no other relationship to the Czech Republic. Such a person is registered only with the administrator of the system administering legal relations to real estate (cadastre). This situation becomes a serious problem when a person who is registered in only one system requests additional services in other systems, typically for the payment of taxes. Thus, in different systems, data is kept for the same person and it is not possible to share data using a reference interface, because it does not exist in the basic register.

For this purpose, the so-called Register of Other Natural Persons was created to collect data on subjects who have interaction with the Czech public administration and then edit these data in the basic register of residents through the foreigners' information system.

Any AIS administrator who registers a subject who is not in the basic register is obliged to:

```
<ol style="list-style-type: decimal;">
```

```
<li>
```

>

```
<p>
```

Find out as much information as is available about the subject. But at a minimum, the first name, last name, date of birth, number and type of identification document.

```
</p>
```

```
</li>
```

</ol></HTML>

```
<ol start="2" style="list-style-type: decimal;">
```

```
<li>
```

>

```
<p>
```

Edit this information into the Other Natural Persons Records system.

```
</p>
```

```
</li>
```

</ol></HTML>

```
<ol start="3" style="list-style-type: decimal;">
```

```
<li>
```

>

```
<p>
```

Ensure that the data in the Register of Other Individuals is updated if the AIS Administrator is notified of it.

```
</p>
```

```
</li>
```

</ol></HTML>

Identifiers of legal persons and natural persons engaged in business

The situation is immeasurably simpler for legal entities and entrepreneurial natural persons that are formed and registered within the Czech public administration. The vast majority of legal persons are recorded in the Register of Persons, which is not subject to such data protection measures because, unlike the personal data and special category of personal data (formerly known as sensitive personal data) of specific natural persons, most data on legal persons is public by nature.

Nevertheless, the use and exchange of corporate data must follow the right principles and use the right identifiers:

- The basic identifier of a legal entity is the identification number (IDN), This is also the primary identifier held within the Register of Persons, where it is also created.
- If a legal entity or an individual has an establishment registered under the Trade Licensing Act, the primary identifier of the establishment is the establishment identification number (OIN), which is also maintained within the Register of Persons.

When a legal person contacts the public administration, it is not in fact the legal person that acts, but a specific natural person acting on its behalf. Even if several legal entities are merged, a natural person acts as a result. The latter must be authorised to do so.

The basic authorisations of specific natural persons are recorded in the Register of Persons as a reference. Specific authorisations for the representation of a legal person may be recorded in the relevant editorial information systems, such as public register systems, and other public administration information systems. The links entered in the Register of Persons are always available within the linked data pool. Other links may be published by a specific AIS, but the reader is always responsible for their interpretation.

Therefore, as communication with a legal person is effectively communication with a specific natural person acting on its behalf, it is imperative that the relevant public authority adheres to the principles of the Personal Data Register in all its related activities.

Subject identifiers are used in official communication and interaction with the client, in the registration of data in the relevant information systems, and in the exchange of data with other information systems.

Evidence of other legal persons

Similarly to the case of registration of other natural persons, a situation arises in the performance of public administration when the services provided do not relate to the entity that is recorded in the basic register of persons. In the framework of the development of the basic registers and thus of the entire PPDF, it is planned to extend the registration of other legal entities.

Any AIS administrator who registers an entity that is not in the basic register is obliged to:

1. Find out the maximum available information about the entity. At a minimum, however, the name, type of establishment and other data on the registration of the legal entity, including tax and other identifiers.

```
<ol start="2" style="list-style-type: decimal;">
```

```
<li>
```

```
</p>
```

Ensure that the data in its data pool is updated, if notified by the AIS administrator, and that the change is subsequently propagated to the records of other legal entities.

```
</p>
```

</HTML></li></HTML></ol></HTML>

When registering entities in the Authority's data trunk.

The aim of PPDF and pseudonymisation is to establish a uniform form of identification of an entity when registering it. The hitherto abused persistent identifiers cannot continue to be used, but instead it is necessary to adapt quickly to the obligations of pseudonymisation. Therefore, the following basic principles for the registration of subjects must be respected:

1. The identifier for communication between the different agency information systems is always the AIFO (the AIFO is translated via the ISZR and ISSS services for each communication via the ISZR and ISSS).
2. The AIFO shall never appear in the system and shall not be accessed by the official.
3. The official/client identifier of an individual must not be the AIFO but always the client number for the agency, assigned by the administrator of the agency, which is used as the presented identifier in the AIS and for the official. This identifier must be meaningless, so no other personal data of the individual can be derived from it. The agenda assigning the client identifier must provide services for obtaining it based on the contact identifier or AIFO and vice versa. At the same time, it shall manage the authorisation to use such a service.
4. When interacting with a client (face-to-face meetings at the counter and processing of incoming documents and messages), liaison identifiers such as document type and number shall be used and a one-stop translation service to AIFO and the services of the issuer of the client identifier shall be used to

obtain that identifier.

5. Liaison identifiers are not primarily recorded unless they are also the client number.
6. A person's AIFO must never be provided directly, the translation service from my AIFO to the AIFO of the recipient of the data exchange is always used (this translation is always performed in the ISZR and ISSS without external intervention as part of the service processing).
7. Unless there are specific reasons for doing so, only the AIFO is exchanged during the data exchange and no additional identifiers or personal data are added.

Services for the translation of the current contact identifier shall be provided with an availability level critical - this is the identification of the person. The issuer or administrator of the contact identifier must ensure the historical uniqueness of the identifier and the services providing the translation to AIFO also for historical values of the identifier (for historical values the availability level required is the primary service).

When interacting with the client

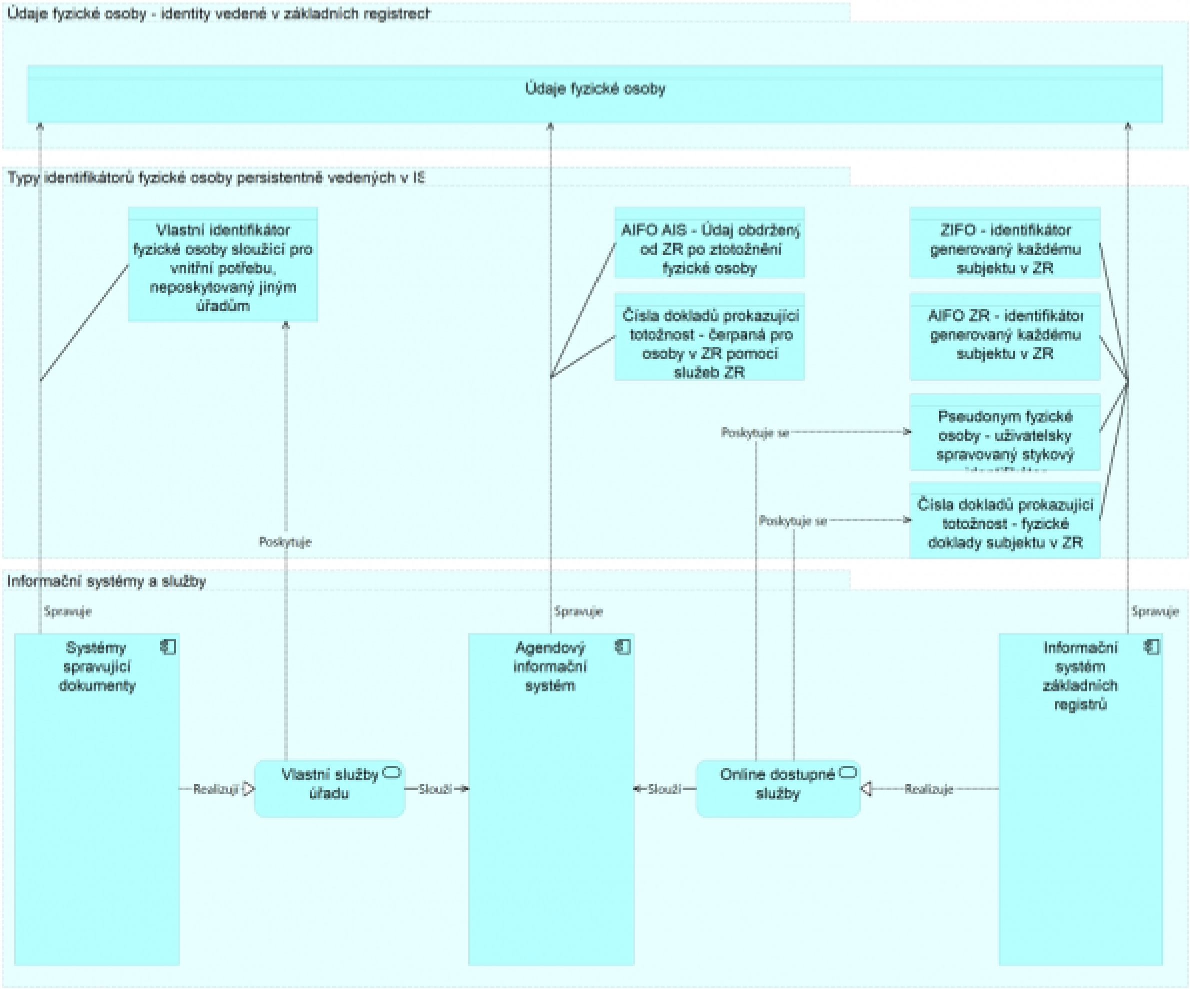
The type and number of the document presented by the client, or otherwise verified contact identifier, shall be used when interacting with the client in person or in person.

- The client shall present a document with a stated identifier that is a liaison identifier.
- A one-time identification service shall be called through the AIS by translating the contact identifier to the AIFO in his/her agenda.
- Furthermore, the official works in the AIS according to the AIFO of the subject (which he does not see on the screen), he does not keep the contact identifier any more. If there is a client identifier, he/she may retain that identifier during communication.
- When communicating with other AIS and other agencies, he/she will use the services of his/her AIS (where the AIS through ISSS will ensure the exchange of data after translation of the AIFO).

When processing forms, the following three situations and resulting procedures then occur:

1. Electronic form: the form must be created in such a way that the identity of the client is already transferred, and during its processing the AIS will perform a trace of the actual data according to the AIFO of the subjects.
2. Paper form: The paper form requires a combination of first name, last name, and document type and number, or other contact identifier. When the form is processed, the appropriate service is called again in the AIS to translate the liaison identifier to the AIFO once, thereby identifying the subject for that AIS. In this case, all data (including identifiers) are remembered because of the need to store the form itself.
3. Assisted filing: In assisted filing at the counter, the relevant staff member will make a present identification against the document and, if acting on behalf of the subject at the counter, will use the relevant services to do so. If he/she is then acting on behalf of the OVM, again when enrolled in the AIS, this AIS will call the one-time translation service of the liaison identifier to the AIFO.

Figure 10: View of identifiers in VS


Údaje fyzické osoby - identity vedené v základních registrech
Údaje fyzické osoby
Typy identifikátorů fyzické osoby persistentně vedených v IS
Vlastní identifikátor fyzické osoby sloužící pro vnitřní potřebu, neposkytovaný jiným úřadům
AIFO AIS - Údaj obdržený od ZR po ztotožnění fyzické osoby
Čísla dokladů prokazující totožnost - čerpaná pro osoby v ZR pomocí služeb ZR
ZIFO - identifikátor generovaný každému subjektu v ZR
AIFO ZR - identifikátor generovaný každému subjektu v ZR
Pseudonym fyzické osoby - uživatelsky spravovaný stykový
Čísla dokladů prokazující totožnost - fyzické doklady subjektu v ZR
Poskytuje se
Poskytuje se
Poskytuje
Informační systémy a služby
Spravuje
Spravuje
Spravuje
Systémy spravující dokumenty
Agendový informační systém
Informační systém základních registrů
Realizují
Vlastní služby úřadu
Slouží
Slouží
Online dostupné služby
Realizuje

Linked Data Pool Standardization

Clear legal definition of data (RPP)

Legally, data is always defined at the level of the provisions of a specific law. Based on such a provision of a specific law, an agenda definition is created and within it a definition of the subject or object whose property is the value of that data.

The definition of the agenda, the link of the agenda to the law, the description of the subject or object according to the provisions of the law, including the breakdown into defined subject data, are stored in the RPP.

Each agenda maintained in the RPP is assigned a unique code which does not change over time. The agenda code is a key identifier in the management of other, legally defined attributes of the agenda. The agenda code consists of the letter 'A' and the numerical designation of the agenda, for example 'A101' corresponds to the agenda 'Basic register - population register'.

Each type of subject or object defined in an agenda (context) is assigned a unique identifier within the RPP. The identifier of the type of subject or object is composed of the numerical designation of the agenda and the numerical designation of the subject or object within the agenda, for example '101-1' corresponds to the subject 'Resident' in the agenda 'A101' - 'Basic register, population register'.

Each subject or object data of an agenda subject or object is also assigned a unique identifier within the RPP. The identifier of an agenda subject or object data is composed of the identifier of the subject or object in the agenda and the numerical designation of the data within the agenda subject or object, for example '101-1-1' corresponds to the data 'Surname' of the object '101-1' - 'Resident' in the agenda 'A101' - 'Basic register, population register'.

The unique identifiers of the agenda, subjects or objects in the agenda and their data as defined in the agenda form the basic legal framework for data transmission on the PPDF reference interface.

The data is therefore always uniquely defined by its code in the RPP. The name of the data is determined by the relevant legal regulation and must not be unambiguous within the linked data pool.

Unambiguous technical data definition - the principle of technical data implemented in the RPP

For every legal definition of a subject or agenda object (SA) data in the RPP, there is at least one corresponding technical definition of that subject or agenda object data. This technical definition is referred to as the Technical Specification of Agenda Data (TSAA) and is maintained in the RPP AIS.

```
__AIS RPP__ is an agency information system administered by the MoI, it is the
primary editing AIS of the RPP base registry.
```

the possibility of having multiple definitions of TSÚA is due to the possibility of versioning the technical specification of the agenda data.

Within the technical specification of the TSA, individual data are defined by data code, name, data, description, data type and additional attributes (e.g. public data, etc.).

Table 5: Attributes that are part of each data

Name	Mandatory	Significance and values	
Status	yes	S - correct	data has correct value
		N - incorrect	the correctness of the data is in doubt, it can only be used as information data
		X - unavailable	the value of the data cannot be determined
		F - incorrect form	the value of the data has been verified as correct by the editor, but the data cannot be stored because it does not satisfy the constraints
date_of_last_change	yes	date and time of the last change to the data value	
date_of_entry	yes	date and time of initial entry of data	
validity_from	no	date and time of the beginning of the validity of the data	
validity_to	no	date and time of the end of the data validity	
Directory	No	Link to a dataset representing a codebook published in the National Open Data Catalogue according to the rules of the Public Data Fund. If the data is created in the agenda, it is a link that says that the data is the source of the codebook, if it is a downloaded data, it is a link to a codebook published by another entity.	

1. *Other circumstances of the change of the data value (author, OVM, reason, ...) must be stored in the change log of the respective system.*
2. *The valid_from value can be lower than the date_of_record value (moving to the address) or higher than the date_of_record value (address for delivery of documents).*

In order to create an agenda data type, the data recorded in the agenda is normalized into a group of logically indivisible objects based on its legal definition within the PPDF. This normalization takes into account both the existing technical implementation in the AIS editors and their ideal technical representation.

The technical specification of the UA, or subject or agenda object data type, is based on the W3C XML Schema Definition Language (XSD) standard.

The technical specification of the AU is performed by authorised users in the AIS RPP. For reasons of clarity, the AIS RPP allows the use of only a limited set of features of the XSD standard. In principle, this is limited to:

1. Simple data types (according to the standard).
2. Complex data types.

Simple data types can be supplemented with attribute type objects.

Complex data types can be supplemented with objects of the attribute, element, sequence and selection types.

Data types are defined in the AIS RPP in the Agency Data Type Catalog (DTAA Catalog), or directly within the agenda data definition.

The administrator of the DTÚA Catalogue is the MoI, Department of the Chief Architect of eGovernment.

The choice of a particular method depends in principle on the evaluation of the general applicability of the data type between different agencies.

Basic common data types

The basic common data types are defined in the AIS RPP in the DTÚA Catalogue.

The basic common data types are defined in global containers that are shared by all Agencies.

Common Core Data Types are created based on a general assessment of the scope of applicability of a particular data type. The definitions of the basic common data types are made by the administrator of the DTÚA Catalogue, and their approval for further use is subject to the approval of the Department of the Chief Architect of eGovernment.

Key Common Core Data Types

The key basic common types are the types that are generally used within the PPDF reference interface. The key basic common types are fixed and are not expected to change.

The selected key common core data types are fixed at XSD level within the Core Registry Information System (RegTypy.xsd).

The following key common basic types, which are also referred to in the remainder of this chapter, include the following types:

- UUID (UuidType) - Universal Unique Identifier.
- CasovaZnacka (CasovaZnackaType) - date and time.
- AIFO (AifoType) - identifier of the resident in the agenda.

- BSI (BsiType) - meaningless identifier of a natural person.
- ID (IcoType) - identifier of a legal entity or a natural person doing business.
- IČP - identifier of the establishment
- KodOvm (KodOvmType) - identifier of the OVM or SPUU.
- KodAgendy (KodAgendyType) - identifier of the agenda.
- KodAdresniMisto (KodAdresniMistoType) - code of the address place.
- AddressLocation (AddressLocationType) - identifier of the address unit.

The reason for introducing basic common data types is to ensure compatibility, interoperability and logical linkage between identical types of data within different systems.

==== Agenda object data

Within the technical specification of an agenda data, the technical representation of each specific data is defined. The technical representation must, to the maximum extent possible, affect the decomposition of the data into its indivisible elements.

The process of decomposition of the agenda object data is a key process in the standardisation of the linked data pool.

The decomposition of the agenda object data must always take into account the existing data types defined in the global containers in the DTUA Catalogue.

Operational Data

Related operational data may be defined within the technical specification of the agenda data.

The placement of operational data within the technical specification is defined by the agenda manager based on the logical granularity of the data.

Examples of operational data are:

- The date the value of the technical data was last changed.
- The identifier of the last change.

Operational data is never kept separate within the data definition, it is always tied to a specific data published by the agenda.

When defining the operational data of an agenda object, the existing data types defined in the global containers in the DTUA Catalog must always be taken into account.

Explicit definition of the meaning of data at the conceptual level of contexts

The legal definition of data stored in the RPP is an overview of contexts and their data held in agendas. The technical side of the data definition then describes the syntactic expression of the contexts in the form of XML schemas. The definition of the meaning of the data is expressed in the form of conceptual models at the conceptual level. It is expressed in the structured form of semantic constraints of the element representing the data in the conceptual model on:

- factually related elements in the same conceptual model,
- factually related elements in conceptual models of other factually related contexts,
- public administration ontology,
- defining provisions of legislation,

- related external vocabularies and ontologies (e.g. EU ISA2 Core Vocabularies).

The definition of each legal data recorded in the RPP is linked to the corresponding element or elements of the relevant conceptual model through their IRI. For each data recorded in the RPP, it is thus possible to identify which element or elements in which conceptual model it corresponds to. Through the IRIs of these elements, a full machine-processable definition of the meaning of the data can be obtained.

The conceptual model is expressed in a machine-processable form. The machine-processable form is technically based on the RDF model of the W3 consortium and is expressed using the RDF Schema and Web Ontology Language (OWL). Semantically, it is based on the Unified Foundation Ontology (UFO).

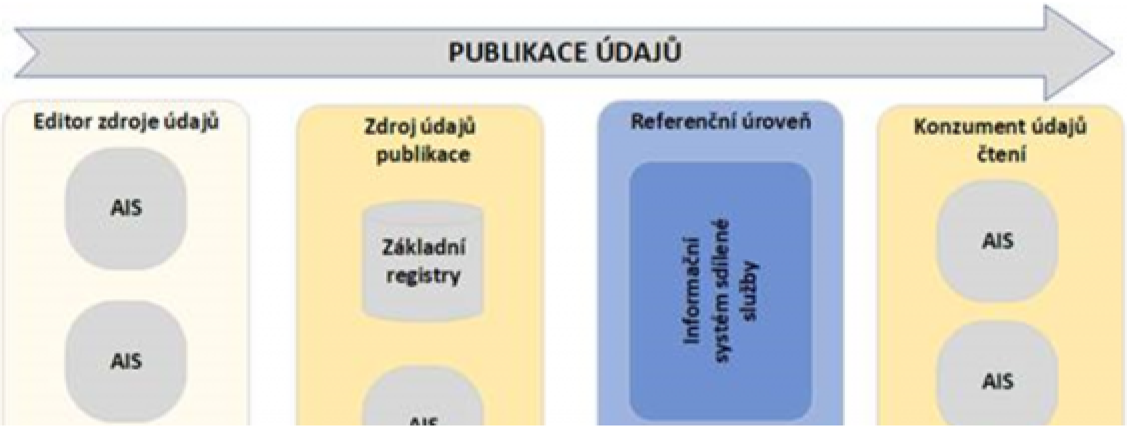
The conceptual models are stored in a separate Conceptual Model Repository, which is a graph database built on the RDF model. Each conceptual model and each element of it is uniquely identified by its IRI in the form of a URL, which also allows a machine-processable form of the conceptual model or element to be retrieved via an HTTPS request. The repository also offers a service for database querying over conceptual models. Technically, this API is in the form of a SPARQL endpoint, i.e. a web service allowing querying in the SPARQL language defined by the W3 consortium. This querying can be combined with querying over the complete public RPP content published as open data also via the SPARQL endpoint. In the same way, it is also possible to combine querying with the content of the eCollection, which makes legislation available in a structured form of individual legal provisions and their hierarchical context through a SPARQL endpoint.

The administrator of the Conceptual Model Repository is the Ministry of the Interior, Department of the Chief Architect of eGovernment. It is also the administrator and substantive guarantor of the public administration ontology. Conceptual models of contexts are developed by the notifiers of agencies and stored in the Conceptual Model Repository. The Ministry of the Interior, Department of the Chief Architect of eGovernment provides a freely available Conceptual Context Modelling Tool and a Conceptual Context Modelling Methodology for the creation of conceptual models. Furthermore, it checks the required quality of the conceptual models delivered to the Conceptual Model Repository and their links to the data definition records in the RPP and requests the necessary correction of the identified deficiencies from the reporting agencies.

Detailed description of the data update process - roles and mandatory procedures

The process of updating data published on the reference interface is based on a general architectural schema describing the principle of operation of the linked data pool.

Figure 11: Working principle of the Linked Data Pool



Two key roles are defined in this process:

1. Data Editor.
2. Data Publication Manager.

The Data Editor is responsible for editing the data in the AIS editor (level -2 - AIS editor). He/she edits the data promptly and is responsible for promptly propagating the data change information and the changed value to the data publishing AIS on the reference interface (level -1 - AIS publisher). The data editor is responsible for the accuracy of the data.

The data publisher on the reference interface is responsible for receiving the change information of the data published on the reference interface from the editor's AIS and publishing it without delay on the reference interface, including publishing the change information in the context concerned. The publication manager is responsible for ensuring that the data is published unchanged.

The data editor is further responsible for implementing the process of communicating a change in the data from the editor's AIS to the publisher's AIS. The definition of the mutual technical interface between the editor's AIS and the publisher's AIS is the responsibility of the publication manager, and is usually based on mutual agreement between the editor's AIS and the publisher's AIS.

The interface between the editor's AIS and the publisher's AIS must adhere to the following principles when implemented:

- Each change has a unique change identifier - the recommended UUID data type.
- Each change has a change date attribute in the AIS editor - the recommended CasovaZnacka data type.
- Each change contains a unique identification of the changed data according to the definition of the agenda data in RPP, i.e. the change can affect multiple data, but always only one object / subject.
- Each change contains an unambiguous identification of the AIS editor so that this information can be handled by systems at higher levels, i.e. so that at each level it can be seen where the source of the data change is.

Detailed description of the process of reading data - where and how the shape and permissions are sourced

The data reading process is always performed on the PPDF reference interface.

Read identification

The data reader must always be identified in the scope:

- Code of the drawing agenda and activity role.
- Code of the drawing OVM or SPU.
- Code of the AIS that is performing the reading.

This identification will be used to verify the authority to read the data.

The reader must identify the agenda data they wish to retrieve as part of the reading process. The agenda data is identified by its unique identifier in the agenda data definition.

When reading, the reader shall be required to provide additional operational information:

- Query identifier in the reader's AIS.
- The reason or purpose for reading the data.
- Clear identification of the entity using the data or to whom the data is provided (identification is the BSI or the VS point of contact).
- Identification of the user who initiated the reading.

The User identification is meaningless in terms of its content on the reference interface, however, it is the responsibility of the AIS administrator to ensure that user identifiers (including history) are recorded in such a way that:

- Comply with the Cybersecurity (IdM, etc.) Decree
- The user's link to the activity roles according to the RPP is recorded.

in the case of user access via AIS using JIP for user authentication, the recommended user identifier is the user's user identifier in the JIP.

On the PPDF reference interface, the above operational information is logged when accessing data. This logged data access information transmitted via the reference interface is provided to authorised entities within the PPDF reference interface.

Checking permissions

Permissions on data published on the reference interface shall be checked against the permissions on data extraction that are maintained in the RPP.

The checking of the permissions to access data on the reference interface is always done before the actual access to the requested data, the access to the data is done after the permissions have been checked. In the event of an attempt to access data for which there is no authorisation, the functionality of the reference interface shall ensure that the entire request is rejected (even if there is authorisation to read other data within a particular request).

The reference interface will not allow reading without specifying the data requested by the reader (i.e. there will be no possibility of drawing according to implicit permissions, reading according to the maximum range of permitted data according to the RPP), taking into account legislative restrictions (e.g. GDPR), where only the set of data necessary for a specific action in the agenda should be used.

Types of permissions

As part of the data reading process, read permissions are essential. The existing read permissions in the RPP are:

- R - reading the current state of the data
- RH - read current and historical data state

In RPP, there are also write permissions for data (W) and write permissions for history (WH), these permissions imply read permissions including history (RH).

In addition to the above permissions, the issue of the volume of data released, typically in situations where searches are performed by data (i.e. not for situations of reading by unique object/entity identifier), needs to be addressed with respect to legislation.

From the point of view of the functioning of the reference interface, it is crucial whether the reader has the permission to read the data (i.e. the 'R' permission). However, from the perspective of the publishing AIS, other attributes of the permission are relevant, i.e. whether the reader has permission to read history (or what extent of history the reader has permission to), what volume of data the reader has permission to search, and so on.

The reference interface should therefore ensure that, in addition to verifying read permissions (and possibly rejecting the request), other permission attributes are passed from the RPP to the publishing AIS so that the publishing AIS can take these permissions into account without maintaining this information directly in the publishing AIS.

Data format

The technical form of each specific agenda data held in the RPP, whose value is published on the PPDF reference interface, is defined in the AISP as an integral part of the definition of the agenda and the data held in the agenda.

Therefore, the current technical definition of a specific agenda data published via the PPDF reference interface is available at any time.

Versioning the technical form of an agenda entry

The versioning of the technical specification of an agenda entry is always relative to the specific moment at which it was approved. If a change to the technical specification is requested, a new version of the technical specification can be created in the AISP, following the XSD versioning principle.

For each version of the technical specification, AISP provides the consumers, which are mainly the AIS readers, with a comprehensive definition of the XSD type corresponding to the published object on the PPDF reference interface.

Operational details

Operational data may be maintained within an AIS publishing data on the PPDF reference interface.

Operational data is related to the object/entity or the agenda data. Operational data is divided into two groups:

- Operational data related to the data value.
- Operational data related to data access.

Operational data related to the value of the data (for example, the date and time of the last change to the object or subject, respectively its data, the identifier of the last change, the status of the data) may be defined within the technical specification of the agenda data in the AIS RPP, in which case they are provided on the PPDF reference interface when the object or subject is read.

Data access-related operational data, i.e. information on who accessed the data, when and for what purpose, is not provided within the technical specification of the agenda data. If this information is provided on the PPDF reference interface, it is provided separately, separately and in a uniform form for all defined agendas and is not bound to the technical specification of the agenda data.

Technical access to the technical specification of the agenda data

Based on the technical data specification defined in the AISP, an XSD definition of the data object/entity is created. This XSD definition is created automatically.

The XSD definition created in AISP is published on the reference interface.

Within the ISSS, the above XSD definition is used to ensure that the technical specification of the data is consistent between the agents and their technical implementation in the publishers' AIS.

Detailed description of the change notification process

The data change notification process is conditional on the data being edited at the data update process level by the data editor.

A change is defined as the creation, modification or deletion of data.

For each object/entity existing within the linked pool, i.e. an object defined in the RPP, a mechanism exists to allow data readers to track changes to the data they are legally authorised to read.

The place through which the reader obtains information about data changes is the reference interface.

The mechanisms related to the change notification process are:

- Login/logout reading of object/entity changes.
- Retrieving changes at a specified interval for logged objects/entities.
- Retrieving changes at a specified interval for a specific subject/object.
- Retrieve change related data.

it is not strictly required to implement all of the above mechanisms for all objects/entities. For example, for the subject - inhabitant in ROB, the unused mechanism is obtaining changes for a specific subject, for the subject - PFO or PO in ROS, on the contrary, subscribing to receive changes.

Obtaining changes means obtaining a list of object/entity identifiers through which data about the changed object/entity can be updated. The actual updating of the object/entity data is done by the process of reading the data.

Receiving change related data means obtaining additional information about the change (change identifier, change date, change type, list of changed data and possibly other, not issued custom data values).

For all of the above mechanisms, the identified reader can generally choose between:

- Changes in any agenda.
- Changes in a specific agenda.
- Changes on a specific data.

To support the change notification process, services supporting the above mechanisms are exposed on the reference interface, again taking into account the suitability for a specific type of object or entity.

For each supported object/entity there is an information system that maintains a list of changes to the data of the subject/object:

- Subject - Occupant - maintained in ROB.
- Subject - PFO or PO - maintained in ROS.
- Object/subject held in RPP - held in ZR.
- Other object/entity - ISSS (e.g. object "Vehicle" in the "Central Vehicle Register", entity "Driver" in the "Central Vehicle Register", etc. The definition of the identifier of the identifier of these objects must be kept in the RPP).

A description of these systems is given in chapter Change Registration System.

An exception to this mechanism is the data held in RUIAN, which has its own system for issuing changes.

Types of changes

Creation / modification / deletion

- of a subject or object.
- Data.

Change notification process strategy

In general, two strategies for data change notification are supported within the PPDF, these are:

- PULL - the reader on his own initiative verifies the existence of changes and reads the list of changes himself.
- PUSH - the reader exposes an interface to which change information is sent from the reference data interface.

For both of these strategies, the reader receives information about changes to objects/entities. Depending on the type of subject/object, this information may include the process of subscribing to changes in specific agendas.

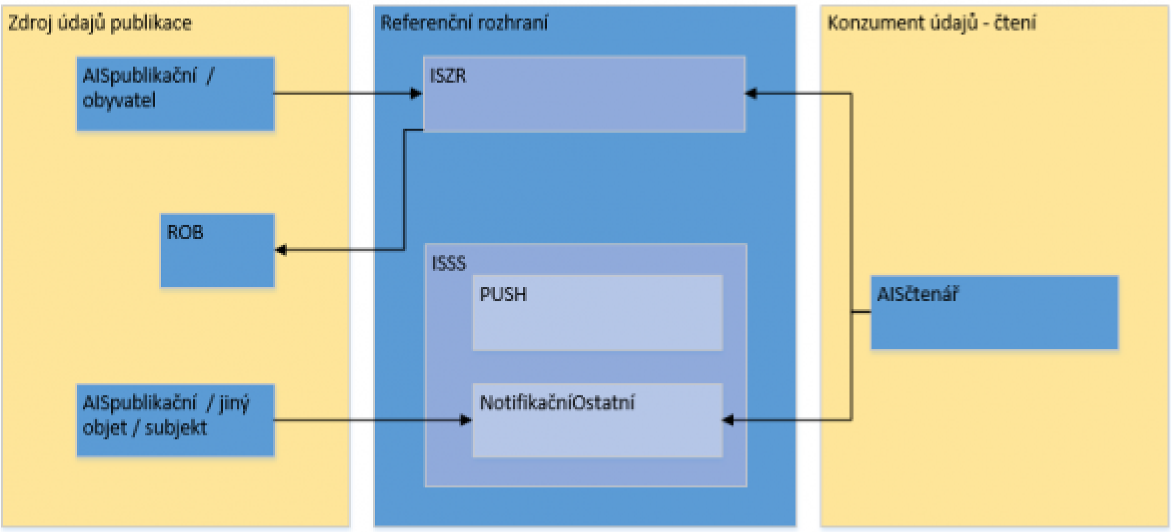
The PULL type strategy is always supported at the PPDF level for all types of subjects or objects. The PUSH type strategy is optional and may not always be supported for all entity or object types on the reference interface.

PULL

Similar to the existing mechanisms implemented in ISZR. The PPDF reference interface exposes services through which a list of changes can be retrieved.

In line with the overview architecture, there is a technical separation of services for extracting changes to reference data held in the RoW and changes to data held in other ISVs (AIS$_{publishers}$).

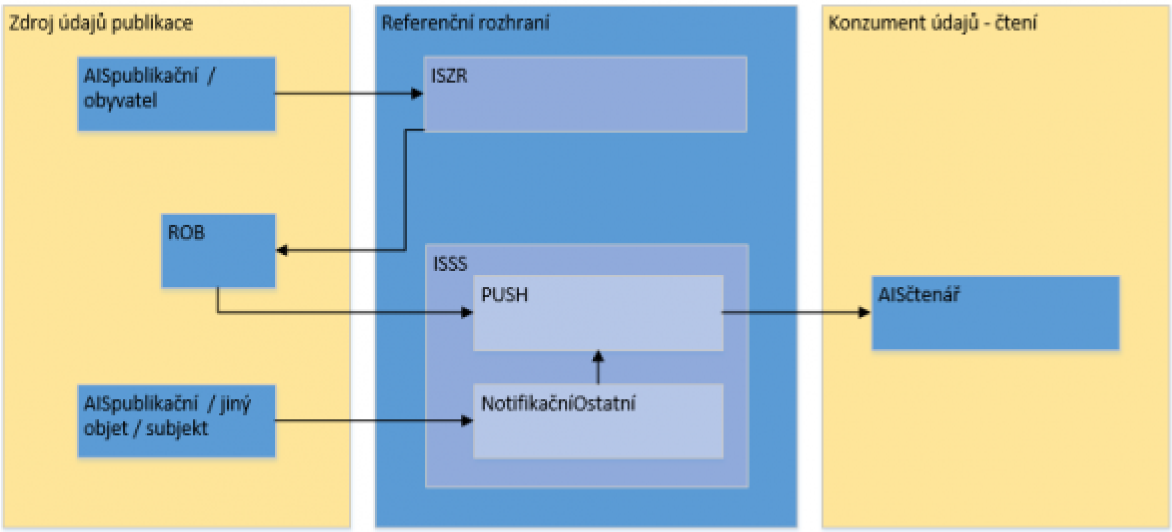
Figure 12: Illustrative use of the mechanism for data in ROB



PUSH

The system maintaining changes for an object/subject whenever a data change is written (insert/delete) via the PPDF reference interface allows to notify the logged in data reader.

When data is changed, the change information for a specific recipient is passed to the reference interface. Endpoints are maintained within the ISSS reference interface for sending notifications to individual readers.



Subscribe to changes

Within the reference interface, there are means for readers to subscribe to read information about changes to object/entity data (and associated means to cancel these subscriptions).

A special case is the creation of a new agenda object/entity. In this case, the reader subscribes to this type of change without specifying a particular object/entity.

Permissions to subscribe to changes

When a reader subscribes to a change subscription, the Reference Interface verifies the reader's permissions for the requested RPP read scope. The Reference Interface will not allow subscriptions to changes that conflict with the current RPP read permissions.

the reference interface shall not output information about changes for which there is no permission at the time of reading the changes; i.e., permission verification is performed against the current state at the time of output.

Change logging system

For all change logging systems, the implementation must be such that the following functionality can be provided, possibly using mechanisms implemented at the reference interface level:

1. The reader will only receive a list of those changes that affect data for which he/she has permission and for which he/she has requested tracking.

Optionally, by object/entity type:

```
<ol start="2" style="list-style-type: lower-alpha;">
```

```
<li>
```

```
</p>
```

When reading changes, the reader will also get a list of data for each object/entity that has been changed in the specified interval.

```
</p>
```

</HTML></li></HTML></ol></HTML>

The _The purpose of (a) is to minimize the reading of data based on change notifications, the result of which would only be to read the state as currently recorded by the reader (since the reader only queries the data for which it has permissions, and that has not been changed). The purpose of (b) is to be able to respond only to changes to specific data that the reader needs to implement a particular process in the agenda.

A fictitious example for (b): the information of procedural interest to AIS is the change of the data "data box" and "account number". The AIS will request to issue changes to these two data. The AIS receives the information that one object has had a change to the 'data box' data and the other object has had a change to the 'account number' data. The AIS may decide that the change to the data box data is not procedurally relevant for the moment and does not need to perform a read for this object via the reference interface, whereas the change to the account number data is relevant for the moment and must perform an immediate read for the other object.

Within the basic registry system, the functionality of the change notification mechanisms as implemented through the eGON services of the ISZR remains independent of the general change notification mechanism.

Within the processes supporting changes and the related change notification mechanisms, rules will be introduced with respect to the possibility of historical reading of changes (a typical example of such a rule is the restriction to obtain a list of changes with respect to the time that has elapsed since the change; one can only ask for changes in the last few days, one cannot ask for changes since the beginning of the century, etc., the length of the period could be addressed individually if necessary).

Subject of law in ROB

The ROB holds reference data on the subject of the residents' data:

- Occupant - subject code according to RPP 101-1.

Support for notification of changes to the reference data held in the ROB for the Inhabitant object of right is directly part of the ROB, the process also includes ORG. The change notification mechanism is handled from both the reader and editor perspective by the eGON services of the ISZR.

Support for notification of changes to data transmitted via the reference interface from publication AIS will be addressed by extending the eGON interface of the ISZR.

The Modification of data that is published via the reference interface:

- The AIS of the editor by whom the edited data on the resident maintained in the ROB is published via the reference interface shall write each change to the published data (data identification according to the RPP) of the agenda maintained by him/her via the eGON service of the ISZR to the ROB.

The eGON EDIS service shall transmit the change data to the ROB after the translation of the AIFO in the ORG. The change information is stored in the ROB on the change repository.

AIS writes: AIFO, time of change, change identifier, list of identifiers of the changed data (data identifier according to RPP, it is linked to the editor's agenda).

The Receipt of a change to the data published on the reference interface:

- The AIS reader calls the extended version of the eGON service published on the eGON interface of the ISZR (PULL).
- The Reader AIS is registered as a recipient of PUSH data change notifications and issues a defined

interface for receiving data change notifications.

As part of the extension of the data change notification process, the Reader AIS will be able to:

- Retrieve a list of AIFOs that have had a change within a defined period. This list will be tied to the AIS login for data change notifications for AIFOs as recorded in the ORG. As part of the request, the reading AIS will need to specify the list of data to be verified for the change to be made.

The introduction of data change notification mechanisms will create additional additional eGON services to address situations that are not yet resolvable or can only be addressed using complex and sophisticated mechanisms.

Within the reference interface it will be possible to:

- Obtain a list of changed data (within the permissions of the drawing agenda) for which a change has occurred for a specific AIFO within a specified time interval. The output of this data will not be linked to the AIFO's subscription to data change notifications.

it is currently not possible to easily verify the existence of changes to specific data for a particular AIFO without reading that data, for example for the purpose of passing it on to others.

- Obtain a list of changes based on the territorial breakdown (with respect to the permissions of the drawing agency). The output will be a list of changes that have occurred within the specified time interval that affect the resident's jurisdiction within the specified zoning area. The output of this data will not be conditional on the AIFO signing up for data change notification.

Simplifying the availability of data now obtained through extracts for municipalities. As part of this change, the consumer will also receive information on the new resident within their territorial jurisdiction.

The consequence of the above description is the necessity to extend the period for which the data on the inhabitant is kept in the ROB, so that it is possible to record changes to the data published on the reference interface for the same period of time that the data is kept by the affected legal entities.

Subject of the right - person in the ROB

In ROS, reference data of the legal entity or natural person undertaking type are kept:

- Person - object code according to RPP 102-1.

Within ROS, changes made to individual entities are currently recorded in ROS for ROS reference data.

ROS will function similarly to ROB in terms of keeping records of changes and supporting the process of notification of changes to data. The data change notification mechanism is handled from the perspective of the reader and the editor through the eGON services of the ISZR.

Support for the process of notification of changes to data transmitted via the reference interface from publication AIS will be handled by extending the eGON interface of the ISZR.

The Modification of data that is published via the reference interface:

- The AIS of the editor by whom the edited data of the entity maintained in ROS are published via the reference interface shall write each change of the published data (data identification according to the RPP) of the agenda maintained by him/her via the eGON service of the ISZR to ROS.

> The eGON EDIS service transmits the change data to ROS. The ROS stores the change information on the change repository, including the identification of the data (according to the RPP) affected by the change.

> The AIS records: ID, time of change, change identifier, list of identifiers of the changed data (data identification according to RPP, is linked to the editor's agenda).

Receiving a change to data published on the reference interface:

- The AIS reader calls the extended version of the eGON service published on the eGON interface of the ISZR (PULL).
- The Reader AIS is registered as a recipient of PUSH data change notifications and issues a defined interface for receiving data change notifications.

As part of the extension of the data change notification process, the Reader AIS will be able to:

- Restrict the reading of changes based on the time interval, the list of data about whose changes the reader wants to receive data, and the identification of ROS entities that are relevant from the reader's perspective (e.g., list of ID number, type of person, legal form, etc.).

In connection with the introduction of data change notification mechanisms, additional eGON services will be created to address situations that are not yet resolvable or that can only be addressed using complex and sophisticated mechanisms.

Within the reference interface it will be possible to:

- Obtain a list of changed data (within the permissions of the drawing agenda) for which a change has occurred for a specific ID (list of IDs) within a specified time interval.

currently it is not possible to easily verify the existence of changes to specific data for a specific ID number without reading the data.

Obtain a list of changes based on the geographical breakdown (with respect to the permissions of the drawing agenda). The output will be a list of changes that have occurred within the specified time interval that affect the resident's jurisdiction within the specified zoning area.

Rights object - entity in RPP

The following data objects/entities are maintained as reference data in the RPP:

- Agenda and agenda execution - object code according to RPP 104-1.
- Right and obligation - object code according to RPP 104-2.
- OVM and OVM category - object code according to RPP 104-3.
- SPUU and SPUU category - object code according to RPP 104-4.

For the Agenda and Agenda Execution object, the operating principle will be similar to the operating mechanism in the RPP.

For the object "Right and Obligation" - it is linked to the AIFO and the ID respectively, with regard to the principle of operation of ROB and ROS, the information on the change must be entered in these ROBs.

For the object 'SPUU and SPUU category' - it is an entity kept in ROS, therefore, with regard to the principle described above, the change must be kept in ROS.

For the object 'OVM and OVM category' - according to the current legislation some OVMs have legal personality and are therefore listed in ROS, but there are also OVMs that do not have legal personality and are not listed in ROS (although an ID number has been reserved for their identifier in ROS, a typical case being municipal districts). This situation can be solved either by introducing a similar mechanism of changes in the RPP or by such a modification of the law that allows keeping all OVMs in ROS and registering changes directly in ROS.

Other objects / entities

For other objects/entities, a mechanism has been created within ISSS to enable the maintenance of a list of changes. ISSS provides:

- Receipt of information about the change of data.
- Promotion of change information.

As part of the data change information receipt mechanism, the publisher's AIS passes information containing:

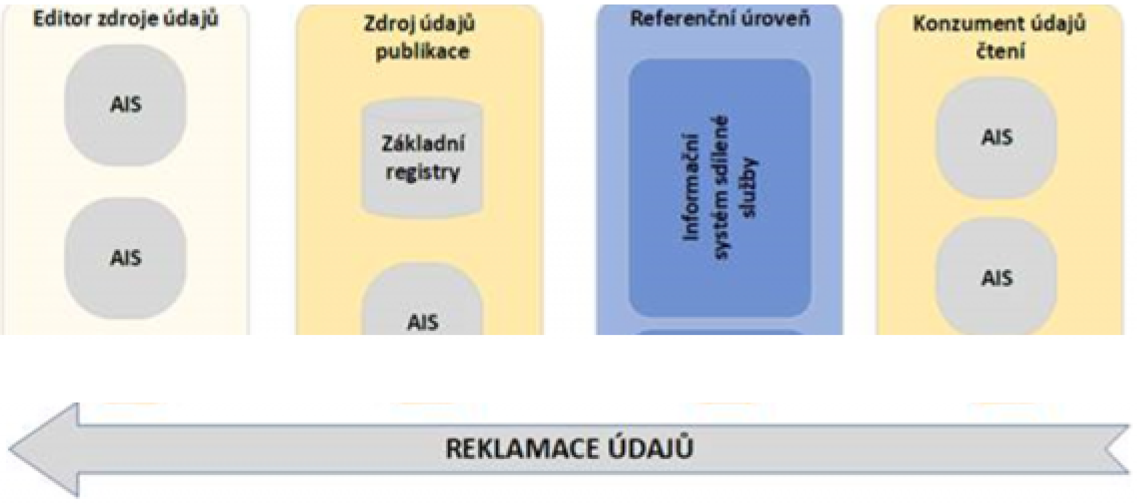
- Identifier of the object/entity changed.
- Date of change.
- Change identifier.
- Change type.
- List of changed agenda data (according to the definition of the agenda data in the RPP).

As part of the data change information propagation mechanism, ISSS stores the transmitted data change information obtained by the data change information reception mechanism in the ISSS repository for providing this information by PULL strategies and simultaneously transmits the change information to the reading AIS.

Detailed description of the data complaint process

The process of claiming data published on the reference interface is based on a general architectural schema describing the principle of operation of a linked data pool.

Figure 14: The process of claiming data published on the reference interface



The data claim process is initiated when the "official", while executing an agenda, finds that the value of the data, which was obtained by reading it through the reference interface, does not correspond to reality.

The described complaint process does not apply to situations where an inaccuracy is detected for a data value that was not obtained through the reference interface (i.e., for example, a data that is processed by an AIS that the 'official' works with directly in the execution of an agenda). This situation should only occur if the executing agenda is also the editor of the incorrect data.

The basic principle of claiming the value of data obtained through the reference interface can be summarised by stating that 'the claim is passed through the reference interface to the left'.

When passing the complaint information towards the editor (i.e., towards the "left"), the source of the complained-of data must be specified within the complaint so that, at any point in time, the processing system will pass the complaint to the system from which it itself drew the information.

A specific situation is reference data maintained in base registries and published through a reference interface. Information about data editors is registered in the ZR, complaints are handled individually on the eGON interface of the ISZR.

The above description of passing information towards the editor is a generalization of the process, a common situation will be a situation where a reader passes a complaint through the reference interface with information about the source system (publisher) and the publisher will also be the data editor.

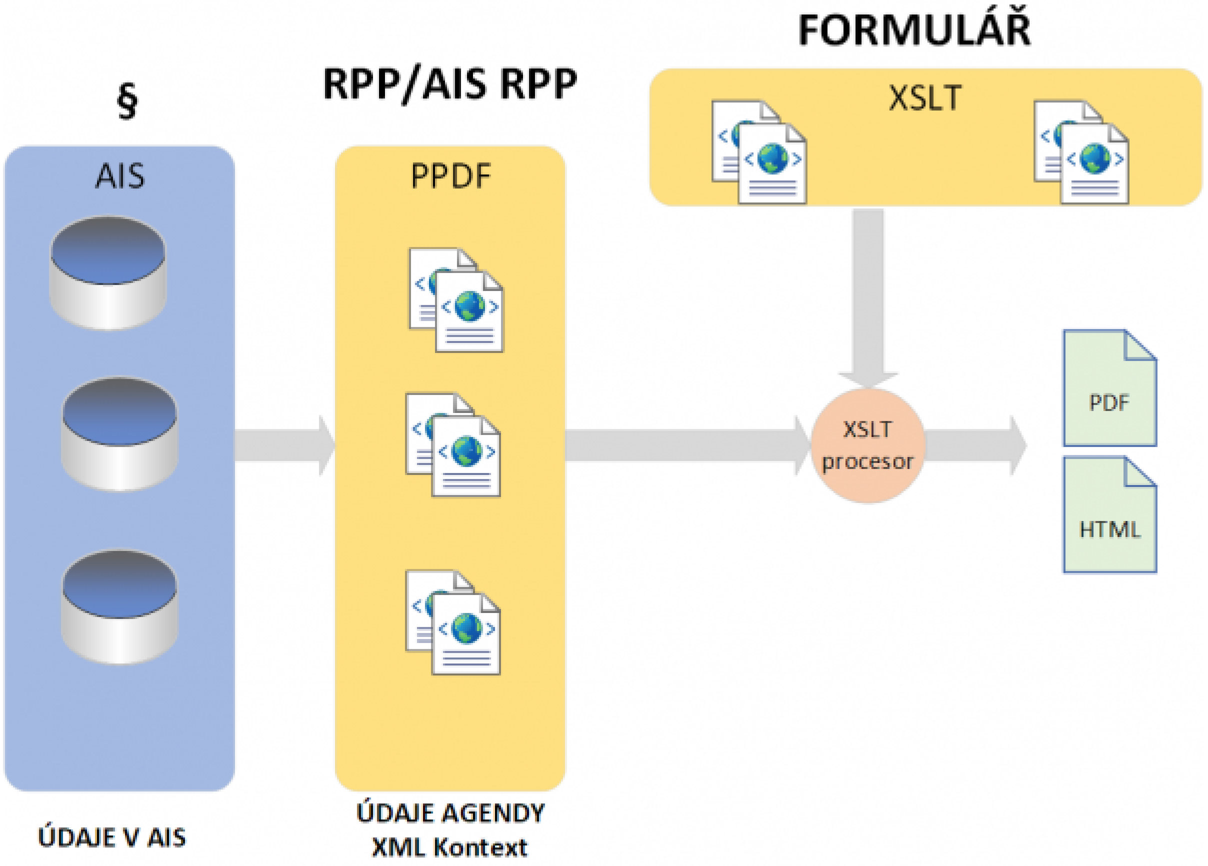
The above description implies that, except for data maintained in the ZR, the consumer of the reading data must process information about the source of the data from which the claimed value was obtained in order to perform the claim through the process described above.

PPDF Presentation (Representation) Standardization - methods and tools used to present data

The presentation or representation of data from a linked data pool converts a technical representation in the form of an XML file into a human readable form. This form of presentation is most often a display on the screen of a client device (HTML and its variants) and a document in PDF form. So far, this task has been seen as a completely independent activity of the individual entities that manage web pages or create PDF documents.

The current process of standardising the representation of data is based on the model forms that accompany the normative texts and determine the appearance of the forms. This process is based on the predominant representation of forms on paper and is currently quite archaic.

The linked data pool allows a completely unambiguous definition and identification of individual data in the form of XSD regulations held in the Register of Rights and Obligations pursuant to Section 54(1)© of Act 111/2009 on the Basic Registers. When presenting these data, it is therefore necessary to define how they will be placed on the form, what description, limitations, etc. they will have. This task is addressed by the W3C Recommendations for XSL Transformation (XSLT) in the current version 3.0 (https://www.w3.org/TR/xslt-30/).



XSLT 3.0 is a language designed to transform XML documents into other representations. Thus, the definition of a form is the setting of rules for transforming the individual contexts (XML documents) that contain the data appearing on the corresponding form. The form thus defined is then uniformly interpreted (represented) when it is used.

The primary definition of the form is therefore the data definition of the form, which will be stored in the Register of Rights and Obligations or the AIS RPP. The use of the form must then respect this stored definition. Each form contains:

- The originator of the form (the public authority that defines it).
- Form ID.
- Form subtype, if any.
- The version of the definition (multiple versions may exist for a single Form ID).
- Validity of the OD-DO version.
- The content of the form definition in XSLT notation.

The form definition (a given version of a given form) uniquely specifies the necessary data sources (data contexts of RPP agendas), their transformation for the given form, the location of individual data within the form, etc. It also specifies any form headers and footers, other graphical elements, and any language versions.

A form may have several subtypes based on the complete form. In a given situation, this subtype containing only part of the complete form may be used.

When processing a form prescription (XSLT definition), the designated XSLT processor creates a representation of the form based on the input XML data and this prescription.

In the case of an HTML representation, i.e. an HTML document on the portal, each portal administrator is responsible for using the current version of the form and using either the complete form or the selected subtype.

In order to ensure a consistent PDF/A-3 representation of forms according to ISO 19005-3, a component will be provided by the Shared Service Information System Administrator to ensure consistent conversion of the XSLT form to the PDF/A-3 representation. This component will therefore produce the corresponding PDF/A-3 based on a request from an authorised entity (having the appropriate permissions to retrieve data within the necessary data contexts required by the form). The authorised entity then processes the created representation, i.e., time stamps, qualified seals, etc., if applicable. It is therefore the functionality of a "universal PDF/A-3 printer".

Mandatory additional processes

Data handling rules

Working with data of natural persons

Act No. 111/2009 Coll., on basic registers, obliges information systems to use a non-public agenda identifier of a natural person (hereinafter referred to as AIFO) when communicating with basic registers - see § 8, paragraph 5. Such communication ensures that the subject of the right is unambiguously identified.

The AIFO shall be assigned to the natural person by the primary ROB editor. The IS of the primary ROB editor shall ensure that the AIFO is assigned to the person only at the moment when the right holder enters the ROB. It shall also ensure that when communicating with other ISs within the ISSS, it never issues an AIFO of an individual it has not yet entered into the ROB.

In order to use the AIFO by another information system, it must first obtain it. This is done by identification, i.e. by searching for the person according to the known data associated with the person, either in the ROB, in the agenda of the primary ROB editor, i.e. in AISEO, AISC or EJFO, or in another agenda enabling an unambiguous search for the natural person. It is most advantageous to use unambiguous data or unambiguous combinations thereof, for example, document number and type, data box identifier, BSI meaningless routing identifier, serial number of a qualified certificate, combination of first name, surname or maiden name and date of birth, birth number, first name, surname or maiden name.

In all cases, the response shall contain the AIFO of the person - if the user is confident that the person has been located correctly, the user shall confirm the identification of the person in their system and store the AIFO in their information system. The AIFO is included in the search response only if it is held in the ROB.

The AIFO is non-public data and the information system administrator is obliged to protect it accordingly.

In order for the information system to use the data change notification service, each AIFO must subscribe to the data change notification service (using the orgSubscribeAIFO service). The data change notification system uses this subscription to filter out unsubscribed AIFOs from the list of changes, so that only the list of AIFOs whose changes have been subscribed to is then fed to the information system. The general process of notification of data changes is described in section 3.5.

If a situation arises where the right holder is no longer the subject of processing in the information system, the system administrator is responsible for unsubscribing the AIFO from data change notifications (using the orgOdhlasAifo service). Discontinuing the subscription to the notification of changes to data prevents unnecessary and unjustified use of the subject's data.

Data obtained by the information system without the use of AIFO cannot be considered as a reference, even in the case of an unambiguous response from the queried system.

Working with data of legal persons and natural persons engaged in business

Legal persons and natural persons engaged in business are uniquely identified by means of a personal identification number (PIN). Unlike the AIFO, the ID number is public data. For natural persons engaged in business, the identification number is to be firmly linked to the AIFO of the business person and that this link is unambiguous.

Typically, natural persons in the ROS are kept just by means of the AIFO and their data are kept by means of a reference link to the ROB. This is the data name, surname and residence address. In cases where the natural person is not listed in the ROB, the name, surname and address of residence can be entered in text in the ROS instead of the AIFO. This necessity should disappear when it is possible to enter such a natural person in the EJFO.

ROS allows searching for an ID number by data as well as by AIFO.

It is possible to receive notifications of changes to data based on the AIFO. In general, the process of data change notifications is described in chapter 4.5. ROS data change notifications are made on the basis of the login/unsubscription of an ID number for data change notifications (rosPrihlasIco / rosOdhlasIco).

If a situation arises where the PIN is no longer subject to processing in the information system, the system administrator is responsible for unsubscribing the PIN from the data change notification service (rosOdhlasIco). By unsubscribing from the data change notification, unnecessary and unauthorised use of the person's data from ROS is prevented.

The data obtained by the information system without the use of an ID number cannot be considered as a reference, even in the case of an unambiguous answer.

Transaction logging rules

Legislative requirements

Decree No. 53/2007 Coll., on the reference interface, in Article 3(3), provides for the obligation of the public administration information system performing the binding to create binding records.

The records include:

1. identification of the public administration information system requesting the service or information,
2. the time of receipt of the request for the service or information,
3. the unique identifier of the requesting system,
4. the structure of the data transmitted and the technical fingerprint of the data values (HASH),
5. information on whether the service or information has been provided to the public administration information system.

Act No. 110/2019 Coll., on the processing of personal data, imposes, in relation to the GDPR Regulation, in Article 36, the obligation on the managing authority to keep records of at least the operations of collection, insertion, alteration, combination, consultation, transmission, communication and deletion of personal data. The records of the operations of collection, insertion, consultation or disclosure allow to identify and verify the reason and time of these operations, the identity of the person carrying out the operation and the identity of the recipient. The records shall be kept for 3 years after the erasure of the personal data to which they relate.

Act No. 111/2009 Coll., on the basic registers, as amended by Act No. 12/2020 Coll. on the right to digital services and amending certain acts.

Pursuant to the provisions of Sections 18(5) and 19(5) of the Basic Registers Act, as amended with effect from 1 February 2022, the Population Register shall keep operational data on the use or provision of data from the Population Register.

The records shall include:

1. agenda code,
2. the code of the agenda information system through which the data were used,
3. the username of the natural person who is the holder of the role, which shall be non-public,
4. an indication of the entity for whose purposes the data are used or provided,
5. the date and time of the use or provision of the data,
6. the business name or the name or the first and last name, if any, of the entity to which the data are provided pursuant to a request under Section 58a,
7. the date and time of the granting or withdrawal of the right holder's consent to the disclosure of data pursuant to Section 58a,
8. the identifier of the consent,
9. the agenda identifier of the natural person for the population register whose data are used or provided,
10. the reason and the specific purpose of the access to the population register.

Pursuant to the provisions of Section 26(4)(e) of the Basic Registers Act, effective from 1 February 2022, the Register of Persons shall keep operational data on the use of data from the Register of Persons.

Pursuant to the provisions of Section 57(2) of the Basic Registers Act, a public authority that has been registered for the performance of an agenda shall keep records of access to data contained in the basic registers, unless the access is to publicly accessible data, and shall keep them for a period of 2 years.

The records shall include:

1. the username of the natural person who is the role holder and who made the access,
2. the role in which the natural person made the access,
3. a list of the data accessed by the natural person who is the role holder,
4. the date and time of access,
5. the reason and the specific purpose of the access.

Pursuant to the provisions of Section 57(2) of the Basic Registers Act, effective from 1 February 2022, the Ministry of the Interior shall keep records of access to data contained in the basic registers, unless the access is to publicly accessible data, and shall keep them for a period of 2 years.

The records shall include:

1. the agenda information system,
2. the agenda code,
3. the user name of the natural person who is the role holder,
4. an indication of the entity for whose purposes the data are used or provided,
5. the role in which the natural person made the access,
6. a list of the data accessed,
7. the date and time of access,
8. the reason and the specific purpose of the access.

Pursuant to the provisions of Section 7(4) of the Basic Registers Act, effective from 1 February 2022, the Basic Registers Administration shall keep a record of access to data held in the agency information systems for the purposes of managing the shared service information system, unless the access is to publicly accessible data, and shall keep it for a period of 2 years.

The record shall include:

1. the identification of the agency information system,
2. the agenda code,
3. the user name of the natural person who is the role holder,
4. an indication of the entity for whose purposes the data are used or provided,
5. the role in which the natural person made the access,

6. a list of the data accessed,
7. the date and time of access,
8. the reason and the specific purpose of the access.

Pursuant to the provisions of Article 7(5), effective from 1 February 2022, the Basic Registers Administration shall issue a record of access to the data at the request of the person about whom the data are held in the agency information systems. The record of access to data held in the agency information systems shall also be issued in the form of a verified output from the public administration information system.

Law No 12/2020, on the right to digital services

Pursuant to the provisions of Article 11(4) effective from 1 February 2020, the service user has the right to be provided with information on changes to the data held about his/her person or his/her rights and obligations in the basic registers or agency information systems immediately after the changes have been made to the data box. The administrator of the relevant basic register or agency information system shall provide the service user with the information referred to in the first sentence to the extent of the data which it does not use from another basic register or agency information system.

Further logging requirements

Identification of downstream log records

The log records of the individual systems shall make it possible to trace the individual processing steps of a transaction. The querying system must ensure that a unique request ID (GUID) is generated for all its queries. This GUID shall be part of the query at all stages of processing, and in addition a unique interface GUID shall be appended to it in the interface references. These identifiers must be stored in the querying system log, the interface log, and the publishing system log. If the publishing system needs to generate a query to another system as part of the response processing, i.e. a composite transaction is created, it uses the original GUID of the querying agent to query the reference interface (i.e. it does not generate its own GUID).

The reference interface and all other systems must be able to trace the chain of all downstream requests, including all data that the systems are required to log, based on the GUID of the reader, publishing system or reference interface request. This guarantees full auditability of any query to the reference interface.

Obtaining logging information

All services require the completion of requester information. This information is collected in the structure ***ResourceInfo*** and is, with one exception, mandatory. By writing this information to the log, all requirements for the logging of the query portion of the transaction are met. It should be required that the reason and purpose of the query should always be stated specifically, not e.g. by reference to the section of law under which the querier is entitled to the data, but e.g. by reference to the reference number.

Table 6: Structure of ZadostInfo

Attribute of the ZadostInfo structure	**Significance**
RequestTime	Date and time the request was sent
Agency	Agency code according to RPP
AgendaRole	Agenda role that the user uses for access
Ovm	OVM or SPUU
Ais	AIS code (serves as an identity space for identifying the natural person to whom the username in the User field belongs)
Subject	Word description of the subject for which the data is used, in the case of a mediated query it carries the designation of the target OVM/SPUU
User	User name of the person

Attribute of the ZadostInfo structure	**Significance**
ReasonPurpose	Specific reason and purpose of the query
AgendaAgendaId	Agenda/AIS requestGUID
IszrActivityId	GUID of request assigned in ISZR
PreviousRequestId	Previous RequestIdentification (optional)

The reference interface logs all the data listed in the previous table, the list of transmitted data (without specific data values) and the one-way cipher of the transmitted message. The message including the transmitted data cannot be reconstructed from the cipher, but it can be verified that the message submitted is identical to the transmitted message.

The information on the data released and the internal identifiers of the data subjects for all responses shall be based on the information stored in the corresponding information system.

The individual other elements of the PPDF shall log the entire footprint of the message they have issued or received, including the data values. If these logs contain personal data, they shall be stored in encrypted form and access to them shall be logged according to the same rules as for access to personal data. The administrator of the information system is obliged to protect these logs from misuse and alteration and, if necessary, must be able to identify the natural person to whom the username in the log belongs.

If the data is used by an automated process (for example, an automatic update process), the system administrator is responsible for its access to personal data.

For the purpose of proving the data issued (there may be a dispute as to what data was issued from the information system or whether the subject was correctly identified), it is advisable that the information system also stores the full XML of the query and response. However, it should be borne in mind that if the logs contain not only a list of data names but also personal data values, these logs need to be protected in the same way as other personal data during processing.

Reference interfaces and publishing systems must mandatorily audit their logs in order to prevent unauthorised use of personal data and excessive burden on ISVS systems. In particular, this audit should verify:

- Correct completion of the ReasonPurpose field. This item should indicate the specific reason for the use of the data and, except for automated processing of data change notifications, should correspond to the actual action indicated by the user. The item should therefore contain a number of unambiguous values.
- Correct completion of the User. Except for automated processing of change notifications, this field should contain the identification of the users. The item should contain a sufficient number of user identifiers and the number of user queries should match the capabilities of the physical user.
- Providing the correct agenda code. Many AISs are logged to perform multiple agendas, but some are statewide. If a querying local OVM system uses an agenda with a central AIS to query, this is likely to be a misuse of data.
- Proper use of the data change notification system. Typically, data change notifications should be processed only a few times a day and should not read the same changes repeatedly.
- The list of data read should not always correspond to the maximum amount of data that the querying system is entitled to receive. By law, it should only query the data needed to perform a specific action.
- Correct use of AIFO and ID number. The reader should identify the subject and then use the subject's identifier for queries, not re-identify the subject over and over again. Control is possible by monitoring the ratio of usage of each service.

Rules for "probe" - indication of service availability

The Probe service is used to verify that the queried system is operational. The service passes to the interrogator the result of a simple "running/not running" population register diagnostic. For this reason, the service has no input parameters.

Since every PPDF system must store logs as described in the previous section and cannot issue any data without writing them, this service must verify the functionality of the logging system.

Every publishing system providing critical services must indicate in the probe service what mode it is operating in. The options are

- Full operation: normal operation, all services are operational.
- Restricted operation: limited operation, only defined critical core services are in operation.
- Mino operation: the system does not provide services (crash state unless communication is interrupted).

Ensuring interoperability

Dependency on processes outside the reference interface (Single Digital gateway, eDelivery)

Basic registries

Given the importance of basic registers in terms of trustworthy and secure e-government services, the European Commission, in cooperation with Member States, has devoted several studies and documents to this issue [2].

In the context of cross-border public administration services, it considers basic registers as a pillar of eGovernment, as they represent a trustworthy, authentic and authoritative source of information managed by a public administration authority or a mandated organisation. According to *European Interoperability Framework 2.0*, basic registers are reliable sources of basic information on natural and legal persons, concessions, buildings and territorial identification. Subsequently, sources of information on other objects (such as vehicles or roads) are linked to these reliable sources.

The basic registers are a practical application of the "data only once" principle, which contributes to the user-friendliness of the services. Rather than repeatedly requesting the data it holds, public administrations are able to share and reuse it between themselves in the provision of digital services.

Interoperability

Interoperability, or the ability of 2 or more systems to cooperate and exchange data through trusted services, is one of the pillars of not only Czech but also European eGovernment or eGovernance.

Due to technological advances and modern public administration's efforts to fulfil the principle of "digital by default" (i.e. to build digital services in priority where it is inherently possible), more and more services provided to end clients are moving from the physical world to the electronic world and it is necessary to address trusted data exchange and related issues such as electronic identity, secure transmission infrastructure, "only once" principles, etc.

Interoperability is a fundamental *prerequisite* of electronic communication and information exchange between public administrations, inter-departmentally and across borders. It is therefore also a prerequisite for achieving the Digital Single Market. Interoperability programmes in the EU are evolving over time. Initially, they were about achieving interoperability in certain priority areas, then about deploying a common infrastructure. More recently, they have started to address interoperability at a semantic level. Some of the issues that need to be addressed next in order to achieve full public services are governance, regulatory compatibility, alignment of organisational processes and security of access to data sources.

Four levels of interoperability

European Interoperability Framework (EIF) https://ec.europa.eu/isa2/eif_en . This is an agreed approach to delivering European public services in an interoperable way.)) recommends taking into account 4 levels of interoperability - legal (legislative), organisational, technical and semantic - when developing inter-agency and cross-border public services.

For each level, the European Interoperability Framework offers specific recommendations on how to overcome the barriers that inter-agency and cross-border e-service delivery may encounter[3].

European public administration services and interoperability requirements

European public services include all departmental and inter-departmental services with a cross-border dimension that public administrations provide to each other or to citizens and businesses in the European Union. In order to take timely account of cross-border interoperability requirements and potential cross-border digital services, we can draw on information on projects that address or will address, data exchange and services. These include:

```
<ul>
```

```
<li>
```

>

```
<p>
```

Implementation of eIDAS

```
</p>
```

```
</li>
```

```
</ul>
```

> Under the eIDAS Regulation, Member States are required to establish a common framework that recognises electronic identities from other Member States and also establishes their authenticity and security, which, in simple terms, means enabling the exchange of guaranteed identities. In the Czech Republic, guaranteed identity is addressed by the existence of a subject of law in the basic register of population and an object of law in the basic register of persons and the basic register of territorial identification, addresses and real estate.
>
> AS IS status:
>
> The implementation of eIDAS in the national environment at the business layer of the architecture was carried out by the creation of Act 250/2017 Coll. - Act on Electronic Identification. From a technical perspective, then the implementation of the National Identity Authority (NIA), where part of the project is the construction of an international gateway for cross-border identification and authentication of citizens from other EU member states, thus ensuring the use of the various services provided in the country. Furthermore, also the announcement of the electronic identification means at the high level, which is the ID card.
>
> TO BE status:
>
> The next steps will lead to the development of the above mentioned technical means to electronicise services at national level in order to provide as many services as possible within the framework of interoperability to other EU Member States. The legislative changes currently being implemented and the introduction of a catalogue of services will lead to the categorisation of individual services and their

> subsequent provision for cross-border use.
>
> The Ministry of the Interior is the lead agency for this activity at national level.

- **SDG - Single Digital Gateway** [4]

> AS IS status:
>
> Phase 1 of this project is currently being implemented. This involves the provision of information on the various services identified by the project. The technical solution is the building of a catalogue of services into a register of rights and obligations and the subsequent modification for the needs of the SDG project.
>
> TO BE status:
>
> The second stage of the project is then the exchange of individual data for the defined services of the SDG project. For the data exchange it is planned to use a technical solution based on the AS4 communication protocol.
>
> The Ministry of Trade and Industry is responsible for this activity at the national level from a substantive point of view and the Ministry of the Interior from a technical point of view.

```
<ul>
```

```
<li>
```

>

```
<p>
```

EESSI - Electronic Exchange of Social Security Information

```
</p>
```

```
</li>
```

```
</ul>
```

> AS IS Status:
>
> Currently 3 contact points (access points) are implemented and are connected to the central communication element created by the European Commission. 1. access point is implemented at the Czech Insurers Office, 2. access point is implemented at the Ministry of Labour and Social Affairs and 3. access point is implemented at the Czech Social Security Administration. All access points are ready to receive and send electronic forms. According to the EESSI project, the exchange of forms is still taking place within a limited number of services.
>
> TO BE status:
>
> The technical solution for the exchange of electronic forms for the whole range of services covered by the EESSI project is being developed.
>
> The Czech Insurers' Bureau, the Ministry of Labour and Social Affairs and the Czech Social Security Administration are the national leaders of this activity.

```
<ul>
```

```
<li>
```

>

```
<p>
```

CPSV - Basic Dictionary of Public Services

```
</p>
```

```
</li>
```

```
</ul>
```

> AS IS Status:
>
> Currently, from a business architecture perspective, the 12/2020 Act - the Digital Service Rights Act - has been passed, which establishes the environment for the creation of a service catalogue and from a technical perspective, the implementation of the service catalogue into the register of rights and obligations is being carried out.
>
> TO BE status:
>
> The development of the service catalogue is planned to enable the exchange of data related to services within the framework of interoperability.
>
> The Ministry of the Interior is the national leader of this activity.

```
<ul>
```

```
<li>
```

>

```
<p>
```

ABR - Access to Basic Registers[5)]

```
</p>
```

```
</li>
```

</HTML></ul></HTML>

> AS IS status:
>
> Basic registries were built in 2012. During this time, they have been continuously developed in the national environment to meet all legislative, technical, architectural and other requirements of the ever evolving government.
>
> State TO BE:
>
> The development of the basic registers is carried out continuously and mainly in response to the development of the ABR project. Interoperability is one of the basic principles at the national level of public

> administration architecture, as evidenced by this and other documents.
>
> The Ministry of the Interior is the lead agency for this activity at national level.

```
<ul>
```

```
<li>
```

>

```
<p>
```

BRIS - Business Register Interconnection System

```
</p>
```

```
</li>
```

</ul></HTML>

> ASIS Status:
>
> At the moment the business registers of all EU member states are already linked (available from url: https://e-justice.europa.eu/content_find_a_company-489-cs.do?clang=cs). Here it is possible to search and view all the basic information about companies and their respective charters (some countries have free downloads of charters, some for a fee).
>
> State TO BE:
>
> In the future, the European Commission wants to use BRIS in particular also for beneficial owners and information about them. At the same time, work and preparations are underway to update the technology and relevant integrations - the so-called BRIS 2.0.

```
<ul>
```

```
<li>
```

>

```
<p>
```

Electronic interconnection of insolvency registers in the EU

```
</p>
```

```
</li>
```

```
</ul>
```

> AS IS Status:
>
> Currently the Czech Republic is one of nine countries connected to a test version of the IRI (available from url https://e-justice.europa.eu/content_interconnected_insolvency_registers_search-246-en.do). There has been a delay in the project as not all countries have public insolvency registers (some have them for a fee etc.).

> > TO BE state:
>
> Currently the structure of the DB of the ISIR system is being redesigned and the corresponding web services are being modified following the revised API specification of the European e-Justice portal. The changes to the ISIR system are planned to be distributed in June this year.
>
> The Ministry of Justice is the national lead for this activity.

```
<ul>
```

```
<li>
```

>

```
<p>
```

MOSS - Simplifying the VAT Single Point of Sale

```
</p>
```

```
</li>
```

```
</ul>
```

> The General Financial Directorate is the lead agency for this activity at the national level.

```
<ul>
```

```
<li>
```

>

```
<p>
```

ESPD - Single European Procurement Certificate

```
</p>
```

```
</li>
```

```
</ul>
```

> The Single European Public Procurement Certificate (hereinafter also referred to as "SPPD") is a tool aimed at reducing both the administrative and financial burden of participating in a procurement procedure. Through this instrument, individual suppliers can submit a standardised affidavit in order to demonstrate compliance with the conditions of participation, instead of having to submit individual certificates, attestations and other documents (often in different forms according to the specific requirements of the contracting authority). This is intended to facilitate participation, in particular for SMEs or foreign suppliers, who will no longer have to search for models of certificates used abroad. The JEO therefore has the potential to simplify the preparation of tenders for these entities, so that they have a wider opportunity to participate in individual procurement procedures. With this wider participation of suppliers, the contracting authorities are then able to obtain better quality and lower prices. The result should be greater democratisation of the public procurement process and the promotion of free competition within a common European market.

Other EU projects and initiatives:

```
<ul>
```

```
<li>
```

>

```
<p>
```

European e-services card

```
</p>
```

```
</li>
```

```
<li>
```

>

```
<p>
```

Corporate law

```
</p>
```

```
</li>
```

```
<li>
```

>

```
<p>
```

Diploma Supplement and European Credit Transfer and Accumulation System[6]

```
</p>
```

```
</li>
```

</HTML></ul></HTML>

Rules for "formatting" data with respect to interoperability

Any data (unless regulated by a special security or other exception, e.g. Act No. 412/2005 Coll. on the Protection of Classified Information and Security Clearance) exchanged outside the Czech Republic must be reference data or linked to a reference subject or object held in the basic registers and an audit trail must be kept of the exchange.

Links of reference data of the RoW to EU datasets

ISA^2: Within the framework of the European Commission's ISA^2 programme, dictionaries for basic objects and subjects have been defined, see https://ec.europa.eu/isa2/solutions/core-vocabularies_en. The content of these dictionaries is only basic and does not reach the full list of data that needs to be maintained in information systems for subsequent interoperability. Only the SEMIC dictionaries, see here https://joinup.ec.europa.eu/page/core-vocabularies, which are described in more detail in Annex 2, provide a sufficient list.

Requirements for the perimeter of basic registers

Operation and communication: The perimeter of the basic registers, given all the above mentioned facts, will be subject to requirements of a non-stop operation (especially the reading part), which will allow the data interoperability to take place seamlessly in 7x24 mode.

There is currently no instrument or legislative environment for reference data interoperability. Therefore, firstly, legislation would have to be provided to enable the cross-border exchange of reference data and then an AIS would have to be built to serve the cross-border transfer of data, in order to ensure the principle that only an AIS type of information system communicates with the basic registers and hence the information system of the basic registers. The communication infrastructure would be the same as in the case of national communication, i.e. using the KIVS and CMS infrastructure with publication to the European TESTA-ng network.

For the interoperability of non-reference data, there is always some legal regulation of the Czech or European level and VPN tools are usually used for communication via the Internet. It would like to move this procedure as much as possible to the TESTA-ng environment and eliminate communication via the public internet.

It is important to note that the European Commission is the administrator of the TESTA-ng infrastructure and it is used to support applications and services that fulfil a European policy managed by one of the European Commission institutions. If there is an application or service that would like to use this infrastructure and does not meet the criteria above, bilateral negotiations can be entered into.

In addition to TESTA-ng communication, the European Commission now prefers to exchange data using the AS4 communication protocol in conjunction with the eDelivery building block[7)] in combination with eIDAS. Any system that exchanges data across borders using the AS4 protocol should have implemented the Domibus[8)]), where the communication itself is then carried out over the free Internet. In the context of cross-border data exchange, this circumstance is foreseen at national level and steps will be taken to develop an infrastructure that will lead to the establishment of a central component as a shared service within a central service point (CMS) that can be drawn upon by the different institutions without the need for each authority to implement technical means on its side.

Ensuring a uniform UTF-8 text data format with definition of supported blocks (pages)

This paragraph defines the character sets for the transmission of text data and the rules for searching text data held by the Public Administration Information Systems in the Czech Republic (not just public administration information systems as defined in the Public Administration Information Systems Act).

Each administrator of an information system must ensure the correct interpretation of data obtained through the reference interface and transmit data to the reference interface according to this document.

From the point of view of reducing the costs of operation and administration of information systems, we recommend that the storage of data in public administration information systems should also respect these rules so that complex converters from other character sets do not have to be created when communicating via the reference interface.

Thus:

- The entire linked data pool works with this single definition (regardless of the actual way text data is

stored in the information systems).
- PPDF is capable of transmitting the full UNICODE set in UTF-8 encoding and data must be transmitted in this character set.

- The search methods shall be used as described in the document below in the chapter 'Searching for text data'.

Responsibilities of ISVS administrators:

- Data can only be stored in the ISVS in accordance with Government Decree No. 594/2006 Coll. (i.e. the entire string is able to transmit, for example, a Chinese character, but is not allowed to be written because it is in violation of the decree).
- Controls must be in place in the ISVS to prohibit storing separate accents and numbers in text where they do not belong (names). At the same time, special characters must not be stored where they do not belong, see tables below.

Transmission and storage of data

Transmission via reference interface

The Unicode character set and UTF-8 encoding must always be used when transferring data between public administration information systems. The transmitted characters shall be interpreted in this character set. If another character set is also used in the transmission of data, then the must also be specified in the Unicode character set in UTF-8 encoding and the figure so specified shall be the reference. The entry in the other character set is only an additional form of the data and is for information only.

The transmitted data must be normalised to NFC (*Normalization Form Canonical Composition*).

For the purposes of this document, we divide Unicode symbols into:

- letters (indicated by the word LETTER or LIGATURE in the name field),
  - lowercase letters (the word SMALL LETTER or SMALL LIGATURE in the name field),
  - uppercase letters (CAPITAL LETTER or CAPITAL LIGATURE in the name field),
  - Latin letters (the word LATIN in the name field),
  - digits (symbols from the C0 Controls and Basic Latin group with the word DIGIT in the name field), we do not allow the use of characters for fractions, Roman numerals, etc. From block U+2150 to U+218F.
- control characters (selected codes from the C0 Controls and Basic Latin group: U+0000 to U+001F, U+007F to U+009F).

This document defines the treatment of letters and special characters that are not digits or control characters. Digits and control characters are also transmitted in the UNICODE character set in UTF-8 encoding, but no search methods other than direct matching are defined for them.

When transmitting text data, it must be ensured that diacritical marks (see following table) are not used separately. It must also be ensured that no numerals are used in text fields unless they are not allowed in the text field (e.g. for First Name or Last Name) and that there is no frequent confusion between the numeral 0 and the letter O or the numeral 1 and the lower case letter L (l).

Table 7: Diacritical marks overview table

<table>
<tr>
<td>English term</td>
<td>Description ^Example^ |ACUTE |comma above right |Á á | |BREVE |round hook above |Ã ă | |CARON |Hook |C | |CEDILLA |hook under the letter |Ç ç | |CIRCUMFLEX |slash (vocal cord) |Ô ô | |DIAERESIS |consonant, colon above|Ü ü | |DOT ABOVE |dot above |Ż ż | |DOUBLE ACUTE |double comma above |Ű ű | |OGONEK |Occasion |Ą ą | |RING |Ring |Ring |Ů ů | |STROKE |horizontal strikethrough |Đ đ | |TILDE |tilde over |Ã ã | Text Search At least the following methods must be available when searching by text entry * CSAS (Case Sensitive, Accent Sensitive) - case sensitive, respecting national characters (diacritics) - i.e. the text is searched as it is transmitted * CIAS (Case Insensitive, Accent Sensitive) - case insensitive, respecting national characters (diacritics). The following method is recommended * CIASCII (Case Insensitive, ASCII) - case insensitive, transliteration to the basic ASCII character set (codes 0x41 to 0x5A) or substitution of special symbols. Conversion for CIASCII mode is done as follows: * Letters are transliterated according to the LATIN letter table given in Annex 1 by converting them to the letter with the name created by removing the name of the attached diacritical mark and changing SMALL to CAPITAL if necessary. * Ligatures are transliterated by converting the Ligature Transliteration table in Appendix 1. * Letters for which no equivalent is found in the ASCII base set by the procedure in 1.1 are transliterated by the Transliteration of Letters without ASCII Equivalent table in Annex 1. ====== Ensuring availability of services ====== ===== Definition of availability from a customer perspective ===== The provision of reliable services that are offered within the agreed and thus also predicted parameters is a prerequisite for the safe functioning and progressive expansion of eGovernment. To determine the basic parameters of the services, it is crucial to observe: * Availability (systems providing services are available in contracted modes, without outages and with limited downtime). * Confidentiality (information is accessible only to those who are authorised to see it). * Integrity (services are provided so that unauthorised modification of the system and information cannot occur). The availability of data interfaces is crucial for the reliable provision of PPDF services. The functionality and high availability of the reference interface when accessing general data stored in the PPDF is one of the cornerstones of the whole eGovernment. Without guaranteed availability of PPDF services, the idea of data sharing cannot be realised. Availability itself can then be understood as the operational reliability of the interface (services are available) and its transactional performance (services are handled with appropriate responsiveness). * Interface reliability - services are available without outages and with limited downtime - is a requirement of the systems architecture - the product of the availability of all sub-systems including supporting assets. * Interface capacity - services are available, handled with adequate responsiveness, and the system allows for</td>
<td>Other^Natural persons^Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</table>

<table>
<tr><td>English term</td><td>Description ^Example^ |ACUTE |comma above right |Á á | |BREVE |round hook above |Ã ă | |CARON |Hook |C | |CEDILLA |hook under the letter |Ç ç | |CIRCUMFLEX |slash (vocal cord) |Ô ô | |DIAERESIS |consonant, colon above|Ü ü | |DOT ABOVE |dot above |Ż ż | |DOUBLE ACUTE |double comma above |Ű ű | |OGONEK |Occasion |Ą ą | |RING |Ring |Ring |Ů ů | |STROKE |horizontal strikethrough |Đ đ | |TILDE |tilde over |Ã ã | Text Search At least the following methods must be available when searching by text entry * CSAS (Case Sensitive, Accent Sensitive) - case sensitive, respecting national characters (diacritics) - i.e. the text is searched as it is transmitted * CIAS (Case Insensitive, Accent Sensitive) - case insensitive, respecting national characters (diacritics). The following method is recommended * CIASCII (Case Insensitive, ASCII) - case insensitive, transliteration to the basic ASCII character set (codes 0x41 to 0x5A) or substitution of special symbols. Conversion for CIASCII mode is done as follows: * Letters are transliterated according to the LATIN letter table given in Annex 1 by converting them to the letter with the name created by removing the name of the attached diacritical mark and changing SMALL to CAPITAL if necessary. * Ligatures are transliterated by converting the Ligature Transliteration table in Appendix 1. * Letters for which no equivalent is found in the ASCII base set by the procedure in 1.1 are transliterated by the Transliteration of Letters without ASCII Equivalent table in Annex 1. ====== Ensuring availability of services ====== ===== Definition of availability from a customer perspective ===== The provision of reliable services that are offered within the agreed and thus also predicted parameters is a prerequisite for the safe functioning and progressive expansion of eGovernment. To determine the basic parameters of the services, it is crucial to observe: * Availability (systems providing services are available in contracted modes, without outages and with limited downtime). * Confidentiality (information is accessible only to those who are authorised to see it). * Integrity (services are provided so that unauthorised modification of the system and information cannot occur). The availability of data interfaces is crucial for the reliable provision of PPDF services. The functionality and high availability of the reference interface when accessing general data stored in the PPDF is one of the cornerstones of the whole eGovernment. Without guaranteed availability of PPDF services, the idea of data sharing cannot be realised. Availability itself can then be understood as the operational reliability of the interface (services are available) and its transactional performance (services are handled with appropriate responsiveness). * Interface reliability - services are available without outages and with limited downtime - is a requirement of the systems architecture - the product of the availability of all sub-systems including supporting assets. * Interface capacity - services are available, handled with adequate responsiveness, and the system allows for</td><td>Other^Natural persons^Other</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

<table>
<tr><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></tr>
<tr><td>English term</td><td>Description ^Example^ |ACUTE |comma above right |Á á | |BREVE |round hook above |Ã ă | |CARON |Hook |C | |CEDILLA |hook under the letter |Ç ç | |CIRCUMFLEX |slash (vocal cord) |Ô ô | |DIAERESIS |consonant, colon above|Ü ü | |DOT ABOVE |dot above |Ż ż | |DOUBLE ACUTE |double comma above |Ű ű | |OGONEK |Occasion |Ą ą | |RING |Ring |Ring |Ů ů | |STROKE |horizontal strikethrough |Đ đ | |TILDE |tilde over |Ã ã | Text Search At least the following methods must be available when searching by text entry * CSAS (Case Sensitive, Accent Sensitive) - case sensitive, respecting national characters (diacritics) - i.e. the text is searched as it is transmitted * CIAS (Case Insensitive, Accent Sensitive) - case insensitive, respecting national characters (diacritics). The following method is recommended * CIASCII (Case Insensitive, ASCII) - case insensitive, transliteration to the basic ASCII character set (codes 0x41 to 0x5A) or substitution of special symbols. Conversion for CIASCII mode is done as follows: * Letters are transliterated according to the LATIN letter table given in Annex 1 by converting them to the letter with the name created by removing the name of the attached diacritical mark and changing SMALL to CAPITAL if necessary. * Ligatures are transliterated by converting the Ligature Transliteration table in Appendix 1. * Letters for which no equivalent is found in the ASCII base set by the procedure in 1.1 are transliterated by the Transliteration of Letters without ASCII Equivalent table in Annex 1. ====== Ensuring availability of services ====== ===== Definition of availability from a customer perspective ===== The provision of reliable services that are offered within the agreed and thus also predicted parameters is a prerequisite for the safe functioning and progressive expansion of eGovernment. To determine the basic parameters of the services, it is crucial to observe: * Availability (systems providing services are available in contracted modes, without outages and with limited downtime). * Confidentiality (information is accessible only to those who are authorised to see it). * Integrity (services are provided so that unauthorised modification of the system and information cannot occur). The availability of data interfaces is crucial for the reliable provision of PPDF services. The functionality and high availability of the reference interface when accessing general data stored in the PPDF is one of the cornerstones of the whole eGovernment. Without guaranteed availability of PPDF services, the idea of data sharing cannot be realised. Availability itself can then be understood as the operational reliability of the interface (services are available) and its transactional performance (services are handled with appropriate responsiveness). * Interface reliability - services are available without outages and with limited downtime - is a requirement of the systems architecture - the product of the availability of all sub-systems including supporting assets. * Interface capacity - services are available, handled with adequate responsiveness, and the system allows for</td><td>Other^Natural persons^Other</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

<table>
<tr><td><b>English term</b></td><td><b>Description ^Example^ |ACUTE |comma above right |Á á | |BREVE |round hook above |Ã ă | |CARON |Hook |C | |CEDILLA |hook under the letter |Ç ç | |CIRCUMFLEX |slash (vocal cord) |Ô ô | |DIAERESIS |consonant, colon above|Ü ü | |DOT ABOVE |dot above |Ż ż | |DOUBLE ACUTE |double comma above |Ű ű | |OGONEK |Occasion |Ą ą | |RING |Ring |Ring |Ů ů | |STROKE |horizontal strikethrough |Đ đ | |TILDE |tilde over |Ã ã | Text Search At least the following methods must be available when searching by text entry * CSAS (Case Sensitive, Accent Sensitive) - case sensitive, respecting national characters (diacritics) - i.e. the text is searched as it is transmitted * CIAS (Case Insensitive, Accent Sensitive) - case insensitive, respecting national characters (diacritics). The following method is recommended * CIASCII (Case Insensitive, ASCII) - case insensitive, transliteration to the basic ASCII character set (codes 0x41 to 0x5A) or substitution of special symbols. Conversion for CIASCII mode is done as follows: * Letters are transliterated according to the LATIN letter table given in Annex 1 by converting them to the letter with the name created by removing the name of the attached diacritical mark and changing SMALL to CAPITAL if necessary. * Ligatures are transliterated by converting the Ligature Transliteration table in Appendix 1. * Letters for which no equivalent is found in the ASCII base set by the procedure in 1.1 are transliterated by the Transliteration of Letters without ASCII Equivalent table in Annex 1. ====== Ensuring availability of services ====== ===== Definition of availability from a customer perspective ===== The provision of reliable services that are offered within the agreed and thus also predicted parameters is a prerequisite for the safe functioning and progressive expansion of eGovernment. To determine the basic parameters of the services, it is crucial to observe: * Availability (systems providing services are available in contracted modes, without outages and with limited downtime). * Confidentiality (information is accessible only to those who are authorised to see it). * Integrity (services are provided so that unauthorised modification of the system and information cannot occur). The availability of data interfaces is crucial for the reliable provision of PPDF services. The functionality and high availability of the reference interface when accessing general data stored in the PPDF is one of the cornerstones of the whole eGovernment. Without guaranteed availability of PPDF services, the idea of data sharing cannot be realised. Availability itself can then be understood as the operational reliability of the interface (services are available) and its transactional performance (services are handled with appropriate responsiveness). * Interface reliability - services are available without outages and with limited downtime - is a requirement of the systems architecture - the product of the availability of all sub-systems including supporting assets. * Interface capacity - services are available, handled with adequate responsiveness, and the system allows for</b></td><td><b>Other^Natural persons^Other</b></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

<table>
<tr><td>English term</td><td>Description ^Example^ |ACUTE |comma above right |Á á | |BREVE |round hook above |Ã ă | |CARON |Hook |C | |CEDILLA |hook under the letter |Ç ç | |CIRCUMFLEX |slash (vocal cord) |Ô ô | |DIAERESIS |consonant, colon above|Ü ü | |DOT ABOVE |dot above |Ż ż | |DOUBLE ACUTE |double comma above |Ű ű | |OGONEK |Occasion |Ą ą | |RING |Ring |Ring |Ů ů | |STROKE |horizontal strikethrough |Đ đ | |TILDE |tilde over |Ã ã | Text Search At least the following methods must be available when searching by text entry * CSAS (Case Sensitive, Accent Sensitive) - case sensitive, respecting national characters (diacritics) - i.e. the text is searched as it is transmitted * CIAS (Case Insensitive, Accent Sensitive) - case insensitive, respecting national characters (diacritics). The following method is recommended * CIASCII (Case Insensitive, ASCII) - case insensitive, transliteration to the basic ASCII character set (codes 0x41 to 0x5A) or substitution of special symbols. Conversion for CIASCII mode is done as follows: * Letters are transliterated according to the LATIN letter table given in Annex 1 by converting them to the letter with the name created by removing the name of the attached diacritical mark and changing SMALL to CAPITAL if necessary. * Ligatures are transliterated by converting the Ligature Transliteration table in Appendix 1. * Letters for which no equivalent is found in the ASCII base set by the procedure in 1.1 are transliterated by the Transliteration of Letters without ASCII Equivalent table in Annex 1. ====== Ensuring availability of services ====== ===== Definition of availability from a customer perspective ===== The provision of reliable services that are offered within the agreed and thus also predicted parameters is a prerequisite for the safe functioning and progressive expansion of eGovernment. To determine the basic parameters of the services, it is crucial to observe: * Availability (systems providing services are available in contracted modes, without outages and with limited downtime). * Confidentiality (information is accessible only to those who are authorised to see it). * Integrity (services are provided so that unauthorised modification of the system and information cannot occur). The availability of data interfaces is crucial for the reliable provision of PPDF services. The functionality and high availability of the reference interface when accessing general data stored in the PPDF is one of the cornerstones of the whole eGovernment. Without guaranteed availability of PPDF services, the idea of data sharing cannot be realised. Availability itself can then be understood as the operational reliability of the interface (services are available) and its transactional performance (services are handled with appropriate responsiveness). * Interface reliability - services are available without outages and with limited downtime - is a requirement of the systems architecture - the product of the availability of all sub-systems including supporting assets. * Interface capacity - services are available, handled with adequate responsiveness, and the system allows for</td><td>Other^Natural persons^Other</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

<table>
<tr>
<td>English term</td>
<td>Description ^Example^ |ACUTE |comma above right |Á á | |BREVE |round hook above |Ã ă | |CARON |Hook |C | |CEDILLA |hook under the letter |Ç ç | |CIRCUMFLEX |slash (vocal cord) |Ô ô | |DIAERESIS |consonant, colon above|Ü ü | |DOT ABOVE |dot above |Ż ż | |DOUBLE ACUTE |double comma above |Ű ű | |OGONEK |Occasion |Ą ą | |RING |Ring |Ring |Ů ů | |STROKE |horizontal strikethrough |Đ đ | |TILDE |tilde over |Ã ã | Text Search At least the following methods must be available when searching by text entry * CSAS (Case Sensitive, Accent Sensitive) - case sensitive, respecting national characters (diacritics) - i.e. the text is searched as it is transmitted * CIAS (Case Insensitive, Accent Sensitive) - case insensitive, respecting national characters (diacritics). The following method is recommended * CIASCII (Case Insensitive, ASCII) - case insensitive, transliteration to the basic ASCII character set (codes 0x41 to 0x5A) or substitution of special symbols. Conversion for CIASCII mode is done as follows: * Letters are transliterated according to the LATIN letter table given in Annex 1 by converting them to the letter with the name created by removing the name of the attached diacritical mark and changing SMALL to CAPITAL if necessary. * Ligatures are transliterated by converting the Ligature Transliteration table in Appendix 1. * Letters for which no equivalent is found in the ASCII base set by the procedure in 1.1 are transliterated by the Transliteration of Letters without ASCII Equivalent table in Annex 1. ====== Ensuring availability of services ====== ===== Definition of availability from a customer perspective ===== The provision of reliable services that are offered within the agreed and thus also predicted parameters is a prerequisite for the safe functioning and progressive expansion of eGovernment. To determine the basic parameters of the services, it is crucial to observe: * Availability (systems providing services are available in contracted modes, without outages and with limited downtime). * Confidentiality (information is accessible only to those who are authorised to see it). * Integrity (services are provided so that unauthorised modification of the system and information cannot occur). The availability of data interfaces is crucial for the reliable provision of PPDF services. The functionality and high availability of the reference interface when accessing general data stored in the PPDF is one of the cornerstones of the whole eGovernment. Without guaranteed availability of PPDF services, the idea of data sharing cannot be realised. Availability itself can then be understood as the operational reliability of the interface (services are available) and its transactional performance (services are handled with appropriate responsiveness). * Interface reliability - services are available without outages and with limited downtime - is a requirement of the systems architecture - the product of the availability of all sub-systems including supporting assets. * Interface capacity - services are available, handled with adequate responsiveness, and the system allows for</td>
<td>Other^Natural persons^Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</table>

<table>
<tr><td><b>English term</b></td><td><b>Description ^Example^ |ACUTE |comma above right |Á á | |BREVE |round hook above |Ã ă | |CARON |Hook |C | |CEDILLA |hook under the letter |Ç ç | |CIRCUMFLEX |slash (vocal cord) |Ô ô | |DIAERESIS |consonant, colon above|Ü ü | |DOT ABOVE |dot above |Ż ż | |DOUBLE ACUTE |double comma above |Ű ű | |OGONEK |Occasion |Ą ą | |RING |Ring |Ring |Ů ů | |STROKE |horizontal strikethrough |Đ đ | |TILDE |tilde over |Ã ã | Text Search At least the following methods must be available when searching by text entry * CSAS (Case Sensitive, Accent Sensitive) - case sensitive, respecting national characters (diacritics) - i.e. the text is searched as it is transmitted * CIAS (Case Insensitive, Accent Sensitive) - case insensitive, respecting national characters (diacritics). The following method is recommended * CIASCII (Case Insensitive, ASCII) - case insensitive, transliteration to the basic ASCII character set (codes 0x41 to 0x5A) or substitution of special symbols. Conversion for CIASCII mode is done as follows: * Letters are transliterated according to the LATIN letter table given in Annex 1 by converting them to the letter with the name created by removing the name of the attached diacritical mark and changing SMALL to CAPITAL if necessary. * Ligatures are transliterated by converting the Ligature Transliteration table in Appendix 1. * Letters for which no equivalent is found in the ASCII base set by the procedure in 1.1 are transliterated by the Transliteration of Letters without ASCII Equivalent table in Annex 1. ====== Ensuring availability of services ====== ===== Definition of availability from a customer perspective ===== The provision of reliable services that are offered within the agreed and thus also predicted parameters is a prerequisite for the safe functioning and progressive expansion of eGovernment. To determine the basic parameters of the services, it is crucial to observe: * Availability (systems providing services are available in contracted modes, without outages and with limited downtime). * Confidentiality (information is accessible only to those who are authorised to see it). * Integrity (services are provided so that unauthorised modification of the system and information cannot occur). The availability of data interfaces is crucial for the reliable provision of PPDF services. The functionality and high availability of the reference interface when accessing general data stored in the PPDF is one of the cornerstones of the whole eGovernment. Without guaranteed availability of PPDF services, the idea of data sharing cannot be realised. Availability itself can then be understood as the operational reliability of the interface (services are available) and its transactional performance (services are handled with appropriate responsiveness). * Interface reliability - services are available without outages and with limited downtime - is a requirement of the systems architecture - the product of the availability of all sub-systems including supporting assets. * Interface capacity - services are available, handled with adequate responsiveness, and the system allows for</b></td><td><b>Other^Natural persons^Other</b></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

<table>
<tr><td>English term</td><td>Description ^Example^ |ACUTE |comma above right |Á á | |BREVE |round hook above |Ã ă | |CARON |Hook |C | |CEDILLA |hook under the letter |Ç ç | |CIRCUMFLEX |slash (vocal cord) |Ô ô | |DIAERESIS |consonant, colon above|Ü ü | |DOT ABOVE |dot above |Ż ż | |DOUBLE ACUTE |double comma above |Ű ű | |OGONEK |Occasion |Ą ą | |RING |Ring |Ring |Ů ů | |STROKE |horizontal strikethrough |Đ đ | |TILDE |tilde over |Ã ã | Text Search At least the following methods must be available when searching by text entry * CSAS (Case Sensitive, Accent Sensitive) - case sensitive, respecting national characters (diacritics) - i.e. the text is searched as it is transmitted * CIAS (Case Insensitive, Accent Sensitive) - case insensitive, respecting national characters (diacritics). The following method is recommended * CIASCII (Case Insensitive, ASCII) - case insensitive, transliteration to the basic ASCII character set (codes 0x41 to 0x5A) or substitution of special symbols. Conversion for CIASCII mode is done as follows: * Letters are transliterated according to the LATIN letter table given in Annex 1 by converting them to the letter with the name created by removing the name of the attached diacritical mark and changing SMALL to CAPITAL if necessary. * Ligatures are transliterated by converting the Ligature Transliteration table in Appendix 1. * Letters for which no equivalent is found in the ASCII base set by the procedure in 1.1 are transliterated by the Transliteration of Letters without ASCII Equivalent table in Annex 1. ====== Ensuring availability of services ====== ===== Definition of availability from a customer perspective ===== The provision of reliable services that are offered within the agreed and thus also predicted parameters is a prerequisite for the safe functioning and progressive expansion of eGovernment. To determine the basic parameters of the services, it is crucial to observe: * Availability (systems providing services are available in contracted modes, without outages and with limited downtime). * Confidentiality (information is accessible only to those who are authorised to see it). * Integrity (services are provided so that unauthorised modification of the system and information cannot occur). The availability of data interfaces is crucial for the reliable provision of PPDF services. The functionality and high availability of the reference interface when accessing general data stored in the PPDF is one of the cornerstones of the whole eGovernment. Without guaranteed availability of PPDF services, the idea of data sharing cannot be realised. Availability itself can then be understood as the operational reliability of the interface (services are available) and its transactional performance (services are handled with appropriate responsiveness). * Interface reliability - services are available without outages and with limited downtime - is a requirement of the systems architecture - the product of the availability of all sub-systems including supporting assets. * Interface capacity - services are available, handled with adequate responsiveness, and the system allows for</td><td>Other^Natural persons^Other</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

<table>
<tr><td><b>English term</b></td><td><b>Description ^Example^ |ACUTE |comma above right |Á á | |BREVE |round hook above |Ã ă | |CARON |Hook |C | |CEDILLA |hook under the letter |Ç ç | |CIRCUMFLEX |slash (vocal cord) |Ô ô | |DIAERESIS |consonant, colon above|Ü ü | |DOT ABOVE |dot above |Ż ż | |DOUBLE ACUTE |double comma above |Ű ű | |OGONEK |Occasion |Ą ą | |RING |Ring |Ring |Ů ů | |STROKE |horizontal strikethrough |Đ đ | |TILDE |tilde over |Ã ã | Text Search At least the following methods must be available when searching by text entry * CSAS (Case Sensitive, Accent Sensitive) - case sensitive, respecting national characters (diacritics) - i.e. the text is searched as it is transmitted * CIAS (Case Insensitive, Accent Sensitive) - case insensitive, respecting national characters (diacritics). The following method is recommended * CIASCII (Case Insensitive, ASCII) - case insensitive, transliteration to the basic ASCII character set (codes 0x41 to 0x5A) or substitution of special symbols. Conversion for CIASCII mode is done as follows: * Letters are transliterated according to the LATIN letter table given in Annex 1 by converting them to the letter with the name created by removing the name of the attached diacritical mark and changing SMALL to CAPITAL if necessary. * Ligatures are transliterated by converting the Ligature Transliteration table in Appendix 1. * Letters for which no equivalent is found in the ASCII base set by the procedure in 1.1 are transliterated by the Transliteration of Letters without ASCII Equivalent table in Annex 1. ====== Ensuring availability of services ====== ===== Definition of availability from a customer perspective ===== The provision of reliable services that are offered within the agreed and thus also predicted parameters is a prerequisite for the safe functioning and progressive expansion of eGovernment. To determine the basic parameters of the services, it is crucial to observe: * Availability (systems providing services are available in contracted modes, without outages and with limited downtime). * Confidentiality (information is accessible only to those who are authorised to see it). * Integrity (services are provided so that unauthorised modification of the system and information cannot occur). The availability of data interfaces is crucial for the reliable provision of PPDF services. The functionality and high availability of the reference interface when accessing general data stored in the PPDF is one of the cornerstones of the whole eGovernment. Without guaranteed availability of PPDF services, the idea of data sharing cannot be realised. Availability itself can then be understood as the operational reliability of the interface (services are available) and its transactional performance (services are handled with appropriate responsiveness). * Interface reliability - services are available without outages and with limited downtime - is a requirement of the systems architecture - the product of the availability of all sub-systems including supporting assets. * Interface capacity - services are available, handled with adequate responsiveness, and the system allows for</b></td><td><b>Other^Natural persons^Other</b></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Required Service Availability

Ensuring availability in terms of services provided

From the point of view of a user of Linked Data services (reader, editor), what matters is not the technical expression of service availability traditionally expressed in the form of SLAs, but the actual availability of services including planned downtime. Planned outages are typically not reported as availability violations, but the service is effectively unavailable to the user.

Thus, the service breakdown below is designed specifically from the service user's perspective and has major implications for the architecture of individual service provisioning. If critical availability is to be ensured for a given service, or if it is a primary service, then the technical and application architecture must be designed to ensure uninterrupted service delivery even in the event of planned maintenance.

Therefore, each information system or part of the communication infrastructure involved in the provision of a critical service or a primary service must have mechanisms designed and implemented to ensure fail-safe service provision.

Critical Services

- **Electronic Identification -** reading data from the Population Register, reading data from the ORG converter, the part of the ISZR providing the above services, electronic identification services of the National Point for Identification and Authentication.

Primary services

- **Authentication services - verification** of the Personal Security Code in the ROB, services of qualified administrators according to Law 250/2017 on electronic identification and follow-up services of the National Point for Identification and Authentication
- **PPDF Data Access - Components** ensuring reading of data in the linked data pool, Basic Registry Information System, Shared Service Information System

Secondary Services

- **PPDF data editing - services** for writing, modifying and claiming data in the linked data pool

Additional services

- Extracts
- Asynchronously provided data

Table 10: Availability of services

Type of service	**Availability**	**RTO^Planned downtime**					
				Operation	**Max length**	**Number/year**	**Mode of outages**
Critical services	99.9%	4 hours	24*7	12 hours	2	non-working days only	
Primary services	99.9%	4 hours	24*7	24 hours	3	non-working days only	

Type of service	Availability	RTO^Planned downtime					
Secondary services	99.7%	4 hours	24*7	48 hours	5	non-working days	
Additional services	99.7%	8 hours	24*7	96 hours	5	out of working hours	

Breakdown of PPDF into different areas (core services, high availability services, defined availability services)

PPDF core services

- Electronic Identification - Obtaining electronic identification of a natural person (AIFO) based on data in ROB and National Point (BSI) - **critical services.**
- Data output - Reading data from PPDF - **primary services.**
- Editing data - write/change data in PPDF - **secondary services.**
- Identity verification - authentication services - **primary services.**

Systems providing basic services

<u>Presentation Services:</u>

- Portals - Citizen Portal, Public Administration Portal.
- CzechPoint.
- ISDS.

<u>Interface services:</u>

- ISZR - interface for accessing the RoW.
- ISSS - interface for access to PPDF.
- NIA - National Identification and Authentication Point.

<u>Data Resources:</u>

- Individual RoBs (ROB, ROS, RUIAN, RPP, ORG).
- Identity provider - eveOP, ISDS.
- Publishing AIS - AIS publishing data within ISSS.

<u>Support services:</u>

- KIVS communication infrastructure.
- Central Service Point - CMS.

Figure 13: PPDF systems

Table 11: Systems and services linkages

Type of service	Providing system	Electronic identification	Data issuance	Data validation^Identity verification - authentication services				

Type of service	**Providing system**	**Electronic identification**	**Data issuance**	**Data validation^Identity verification - authentication services**				
Interface services	ISZR - interface for accessing the ZR	Provides	Provides	Provides	Provides	Provides	Provides	Provides
	ISSS - interface for accessing PPDF			ISSS				
	NIA - National Identification and Authentication Point	Provides	Provides	Provides	Provides			
Presentation Services		Portals - Citizen's Portal, Public Administration Portal			PROVIDES			
		CzechPoint			PROVIDES			
	ISDS		MEDIATES					

		Identity provider - eveOP, ISDS				PROVIDES				
	Publishing AIS - AIS publishing data within ISSS		Provides	PROVIDES						
Supporting Services	KIVS Communication Infrastructure	Provides	Provides	Provides	Provides	Provides	Provides	Provides	Provides	
		Central Point of Service - CMS				SUBSCRIBE		SUBSCRIBE		SUBSCRIBE

Ensuring consistency of PPDF

A Linked Data Pool, like any data source, must have precise rules defined for the entire lifecycle of the data maintained. This lifecycle includes the steps of insertion, maintenance and deletion of an individual data or a specific entity (subject or object about which data is held). Without setting and following these rules, the consistency and trustworthiness of the data provided by this data source cannot be ensured.

By definition, data consistency is ensured at the internal level (within a single data source or database) and external or link level (consistency between data sources). From this perspective, the Linked Data Pool must appear to the data reader as a fully consistent system with complete data and link validity.

The basic linkage tool for entities is a reference to the identifier of a natural person (AIFO) in the Population Register or the identifier of a legal person (ID) in the Register of Persons. Within eGovernment, the principle is enforced that all data on subjects of law are kept with a reference link to this reference and if this is not the case (natural person does not have a record in ROB, legal person does not have a record in ROS), then the data on these subjects are only informative and the recipient-reader of these data does not have a guarantee of their correctness and assured relationship to the person.

Therefore, the primary task of ensuring the consistency of PPDF is to ensure the permanent validity of reference links in all information systems of the public administration and private data users according to the Basic Registers Act.

Subsequently, the authoritative originator of each data on a person must be known, i.e. within which agency and agency information system it is created and provided to the linked data pool. It is only from this source that a specific data can be drawn by other readers and considered correct. The same source must also provide tools for the maintenance of the data published by it, i.e. notification of changes to the data and the receipt and processing of data complaints.

Role Definitions

In terms of ensuring consistency of the PPDF, the following basic AIS/OVM roles can be defined, listed according to the natural life cycle of the data:

- **Data Originator -** is a public authority that performs a specific agenda and within that agenda provides the data origination process based on its official activity. It is therefore, for example, the competent municipal authority that establishes the data on the place of permanent residence of a citizen of the Czech Republic. Subsequently, it records this data into the agency information system, which is either another recorder or already ensures its distribution within the interconnected data pool (publisher). In the latter case, the data is entered into the information system of the population register.
- **The data publisher -** ensures the publication of the data in the reference link to the subject of law in the Linked Data Fund as a reference (from the basic registers) or as a data of the agenda information system (authoritative data originator). In the above case, the Population Information System is the editor of the current data on the address of the place of residence in the Population Register or the publisher of the historical data on the address of the place of residence.
- **Data reader -** is a public authority or private data user who, in the performance of an agenda, uses data from the linked data pool provided by the publishers in relation to the subject of law. It may store the data thus obtained in the data base of its agenda (its information system) if it is legally authorised to do so
- **Auditor -** typically the administrator of the basic register or other common publishing system, who does not verify the validity of the stored data, but ensures their syntactic validity (e.g. the occurrence of a digit in a string where only letters should be - substitution of zero 0 and capital O) and the currency of reference links (the subject with the given link exists in the relevant basic register).

It is clear from the above distribution that there may be a whole chain of editors before the data is published to the Linked Data Pool.

In the case of base registries, special roles of **primary** editor and **secondary** editor are defined. Only the primary editor can create, modify (merge or split) or delete a subject right. The secondary editor can then only modify the corresponding entry for an existing right entity.

PPDF Consistency Maintenance Rules

Creation and publication of data

As mentioned above, each PPDF data is created by the action of the relevant public authority and, through a sequential chain of editors, is entered into the Agenda Information System, which publishes the data in relation to the subject or object of the right.

The subject matter manager of the publishing AIS sets the rules for its editors to ensure that the data published by it is secured:

- Correctness - the data is correct to the extent that the editors are able to ensure this correctness.
- Reference linkage - the entry is linked to the correct person by a reference linkage in ROB or ROS.
- Formal correctness - the entry is entered and published in a formally correct manner.

The Subject Administrator ensures that the agenda is correctly reported in the ROB and its AIS. Indicates data that are published as AIS data (i.e., in the agenda - AIS) originate and whose correctness is therefore guaranteed by the execution of its agenda. The AIS technical administrator must ensure compliance with and enforcement of these rules of the subject administrator, including the basis for the technical specification of the data within the AIS RPP, which may include any regulatory checks on the formal correctness of the entry of the data (e.g. there must be no digits or special characters in the data).

The publisher must ensure that the data published by him/her is transmitted to the linked data pool unchanged (as entered by the editor) and that it is used and provided in accordance with the declaration of the relevant agenda in the RPP and its AIS.

Note: for basic registers, this functionality is provided by the Basic Registers Information System.

The subject AIS publishing administrator shall not publish as an AIS data item in the linked data pool a data item that does not originate from the activities of his/her agenda(s) and has been obtained from the linked data pool as a data item from another publisher. Such data may be published as informative only and the publisher shall not be liable in any way for its accuracy.

Reading the data

In the operation of an agenda, data generated in other agendas may be used and stored according to legal authorisations. It should be noted here that the use and storage of data is a different process in terms of data protection. It is possible to use the data in the process of executing an agenda, but it may not be possible to store it further in the agenda information system supporting the execution of the respective agenda.

Data from the linked data pool is primarily retrieved with a link to the relevant entity - AIFO or IČO. Therefore, the reader is responsible for correctly identifying the entity whose data from another agency information system he/she wants to use - transferring the AIFO or IČO. If the reader is not able to identify the subject according to the data known to him/her, he/she can use the service of the publisher, to whom he/she transmits the corresponding data and on the basis of such transmitted data obtains the AIFO or IČO - reading according to the data. In this case, the reader is again responsible for providing the correct data on the basis of which the person is identified. The publisher is responsible for identifying the subject according to the data provided.

The reader must not republish the data it has obtained from the linked data pool as if it were AIS data, i.e. as if it were generated by the activity of an agenda supported by the AIS.

An activity within an agenda may reveal a discrepancy between the data provided by the publisher and the actual state. In that case, the reader is obliged to initiate a claim for such data.

Data Complaints

If the reader of the Linked Data data or the auditor finds a discrepancy between the data obtained and the actual state, then the reader is obliged to implement a claim of such data. He/she shall forward the complaint to the administrator of the corresponding publication AIS, stating the reason for the complaint and, if necessary, a proposal for the correct form of the data according to his/her findings.

The complaint shall be forwarded to the material administrator of the publication AIS. If the administrator of the publication AIS makes available a service for receiving complaints in the linked data pool, the reader is obliged to use this service. Otherwise, it shall follow the Administrative Procedure Code.

After receiving a complaint, the publication AIS administrator forwards it to the relevant editor. Again, if the editor provides a service for receiving complaints, the publisher is obliged to use this service, otherwise it follows the Administrative Code.

Upon receipt of a data complaint, the data editor shall promptly decide whether to investigate the accuracy of the data. In this case, it shall immediately mark the data as incorrect with the publisher and initiate an investigation leading to either confirmation of the data status or its correction. Upon completion of this investigation, the editor shall update the entry and remove the incorrect designation, as appropriate.

It should be noted here that these processes are both governed by administrative rules (in terms of deadlines) and it is in the interest of all participants in the linked data pool that the status of the data is up-to-date and correct. Only in this case can the agencies work efficiently with the data in the PPDF without the need to verify it.

Data Audit

Auditing of data and reference links is carried out by the AIS Publication Manager. It must ensure data and reference link maintenance processes

- Verifying that reference links are up-to-date - AIFOs, IČOs or RUIAN codes refer to an existing entity or object in the basic registers. If a breach of reference links is detected, the publisher identifies the link as incorrect and informs the editor with a request for remedy.
  - The editor handles the correction of reference links according to the rules of his agenda. For example, if the address is an address written by reference to an address point and the last valid address must remain in the agenda, it overwrites it with the text from the last known form of the address. Another example is an individual whose details have already been removed from the ROB. In this case, it retains the person's AIFO (the records in the ORG converter are valid) and records that the person has been removed from the ROB.
- Verification of formal correctness of data - the publisher regularly verifies whether the data entered by the editors are formally correct. This formal aspect is defined by the publisher in the agenda declaration in the RPP and AIS RPP in the Technical structure of agenda data section. In case it detects a violation of the formal correctness of the data, it marks this data as incorrect and informs the editor with a call for correction.

Notification of data changes

Data change notification is a tool to ensure that data on subjects and objects in the information systems of public administrations and private users are updated. The administrators of the individual information systems are obliged to keep up-to-date the data they obtain on subjects and objects from the linked data pool. In order to manage these updates efficiently, all publishers provide a notification service for changes to the data.

Each publisher should therefore provide a data change notification service for the data for which it is the authoritative source. This service provides information to readers about data changes and allows them to obtain the current data.

If the publisher does not provide this service, data readers must periodically update the data they receive by reading the data for the entire tribe of subjects and objects they maintain in their information system. In the event that a large amount of data is updated in this way, the publisher's services will be severely overloaded.

Conversely, if the publisher provides data change notification services, the reader is obliged to use these services to maintain the retrieved data.

Responsibilities of individual roles in verifying reference links

Data on subjects or objects obtained from a linked data pool may be stored in the agenda information system in the form of a reference binding (reference to a record in the underlying registers) or in a so-called dereferenced state (direct entry of the data value).

In the basic registers, the preferred method of storage is the reference link (AIFO, ID number, Address point). In individual AIS, the data can be stored as a reference binding and as a direct dereferenced data value. The decision on how to store the data is based on the procedural rules of the agendas that are executed through the AIS. From the point of view of data protection and data uniqueness, the recommended way is to store the reference binding and the partially dereferenced data (data that are necessary, for example, for searching in the agenda data) simultaneously.

The AIS administrator, and in particular the individual basic registers, must keep the reference links up to date. It must therefore have processes in place to react to the change or termination of a stored reference link. It uses the processes described in the previous chapter to detect these changes. Administrator:

- Provides data change notification services
- Receives notifications of changes to reference links (e.g. split or merge of AIFOs, termination of Address Point)
- Audits the status of reference links
- Arranges for the reclamation of data in the event of a change. In particular, when a reference binding is broken by the disappearance of a referenced object or entity (defunct address point, merged or split AIFO), it marks the binding as incorrect and initiates a claim with the data editor

The registry administrators of the basic registries must provide a service that allows either to obtain the successor of the reference link (the object or entity that replaces the broken one) or the last known value of the data related to the reference link at the time of its breaking. The reader can then replace the reference binding by a direct entry of the last known data.

Legislative changes required

To be developed after comments from all ZR administrators.

ZR Act

- Mechanisms for notification of changes to per capita data in the ROB.
- Period for keeping the document number in the ROB to be extended to the period when the person himself is kept in the ROB - for the possibility of retrospective validation.
- Keeping European regulations and directives in the ROB as a basis for international data sharing.
- Mechanisms for notification of changes to data of legal and natural persons in the ROB.

Follow-up implementation steps

To be elaborated after comments from all RoW administrators.

Annexes

- Annex 1_UNICODE
- Annex 2_SEMIC

[1] Act No. 111/2009 Coll., on basic registers, as amended by other legislation in force on 1 January 2025

[2] e.g. "*Access to basic registers. Examples of good practice in the successful interconnection of basic registers*" (2016): https://ec.europa.eu/isa2/sites/isa/files/publications/access-to-base-registries-good-practices-on-building-successful-interconnections-of-base-registries.pdf

[3] pp. 27-31; and "*Access to basic registers. Examples of good practice for successful interconnection of basic registers*" (2016): https://ec.europa.eu/isa2/sites/isa/files/publications/access-to-base-registries-good-practices-on-building-successful-interconnections-of-base-registries.pdf

[4] http://www.consilium.europa.eu/cs/press/press-releases/2017/11/30/digital-single-gateway-council-agrees-to-make-access-to-information-and-services-easier/

[5]

```
<p>
```

https://joinup.ec.europa.eu/collection/access-base-registries

```
</p>
```

[6]

```
<p>
```

https://ec.europa.eu/education/resources/diploma-supplement_cs and https://ec.europa.eu/education/resources/european-credit-transfer-accumulation-system_cs

```
</p>
```

[7] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Access+Point+specifications SML/SMP technical specifications: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SMP+specifications and https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SML+specifications

[8] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Domibus

From:
https://archi.gov.cz/ - **Architektura eGovernmentu ČR**

Permanent link:
https://archi.gov.cz/en:znalostni_baze:ga_ppdf

Last update: **2021/07/07 15:27**