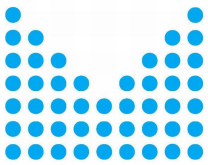
Materiál Ministerstva vnitra



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Export z Národní architektury eGovernmentu ČR

Obsah

Pseudonymisation of subjects in the Interconnected data pool

Pseudonymisation means storing data using the technique of separating agency and identification data and linking them using AIFO according to the above scheme:

Pseudonymization **is not** anonymization of data, and even pseudonymized data is still personal data.

Thus, the purpose of pseudonymization is:

1. To reduce the risk of unauthorised handling of personal data
2. Reduce the risk of unauthorised association of personal data (also referred to as "profiling")

In contrast to the practice commonly used today, where all data about individuals is stored in one table (i.e. including personal data), this is a systematic division of the stored data so that the data is separated from each other at a minimum:

- **Agenda own -** data created within the agenda in which the office is held
- **Referential -** data obtained from the population register or other registers
- **Agenda-specific -** data obtained from other agendas relevant to the given agenda

Legal aspects for pseudonymisation

Act 111/2009 Coll. on the Basic Registers introduced the basic principle of pseudonymisation in public administration in the form of **Agenda Identifier of a Natural Person (AIFO)** (§9 to §11 of Act 111/209 Coll. on the Basic Registers), which ensures pseudonymisation in the performance of public administration. The consistent use of AIFO within the ISVS ensures the reduction of the risk of profiling in the sense of unauthorised linking of data on a specific person from different agencies.

Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as GDPR) defines pseudonymisation in Article 4 as follows:

"*pseudonymisation*" *means the processing of personal data so that they can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is kept separately and is subject to technical and organisational measures to ensure that it is not attributed to an identified or identifiable natural person*

With reference to the above, it should be noted that the currently still used **birth number is in direct conflict with the requirement for pseudonymisation**, since the RIN, in addition to being a meaningful identifier (containing information on the date of birth and sex of the person), in particular allows for the association of any data held in connection with it.

Department of the Chief eGovernment Architect of the Ministry of the Interior

The Ministry of the Interior is, according to Section 12 of Act No. 2/1969 Coll., the Act of Competence, the central authority of the state administration, inter alia, for the ISVS area and also performs a coordinating role for information and communication technologies, as well as for the organisation and performance of public administration in general. These competences are further elaborated in the ZoISVS, according to which the Ministry of the Interior expresses its opinion on proposals, projects and investment plans of the OVS in the field of information and communication technologies.

On the basis of the relevant regulations, the Department of the Chief eGovernment Architect of the Ministry of

the Interior (OHA) performs the described coordination role in the field of information and communication technologies. The OHA has supra-ministerial competence, i.e. it is mandated and responsible for coordinating and leading the development of eGovernment throughout the public administration. eGovernment itself includes not only information technology itself, but also the optimization and simplification of public administration services linked to the legislative environment. In addition to the aforementioned legislation, the OHA is also explicitly called upon to play this coordinating role by Government Resolution No 86 of 27 January 2020.

Pseudonymisation requirements

The requirements for the pseudonymisation of personal data are **architectural, implementation and procedural.** Their implementation must be carried out in such a way as to in no way restrict the exercise of public administration. Ideally, ISVS users should not notice that pseudonymisation processes are used to store and handle personal data.

The specific implementation of this requirement depends on the complexity of the information system and the agendas it supports

Pseudonymisation architectural practices

Pseudonymisation is not an explicit requirement for the processing of personal data, but it is a recommended practice for reducing the risk of unauthorised handling of personal data, along with other techniques such as encryption.

- **Statewide level** - consistent use of the AIFO identifier, through communication with Basic Registry Information System and eGON Service Bus/Shared Service Information System, when exchanging data between ISVs, while avoiding/stopping any exchange of agenda data without the use of AIFO.
- **Local level** - separation of the primary identification data of a person (reference data held in the Population Register) from the data generated within its own agenda, and also separation from data possibly obtained from other agendas on the basis of authorisation in the execution of a specific agenda
- **Agency level**: Ensuring the use of pseudonymised agency identifiers in AIS and the possibility of exchanging data from the Interconnected data pool through the translation of identifiers via ISZR
- **Supplementary measures** - encryption of stored data, which increases the protection of personal data in case of theft of data files (also in the form of backups) and consistent logging of access to personal data

At the national level

At the national level, the introduction of the Basic Registers establishes a secure way of exchanging and managing personal data. Each agenda is assigned an AIFO of a person and only the AIFO converter (ORG) is able to transfer the AIFO of a given person between the different agendas. Each such transfer is consistently logged and the exchange of data is recorded in the population register log.

When exchanging data between agencies, it is always necessary to consider the scope of the data being transferred. In many cases, the current legal framework provides for the authorisation to obtain a large amount of data between agencies in order to ensure the unambiguous identification of the person about whom the data are transferred. It is important to note here, however, that although there may be broad legislative authority to obtain data from the source agency, it is advisable to use only strictly necessary data with regard to data protection.

The use of a valid identification document is ideal for the identification of a natural person when he/she contacts the public administration, since any public authority that uses some reference data recorded in the population

register in its activities is entitled to use the number and type of electronically readable identification documents (§18(5) of Act 111/2009 Coll. on the basic registers). Therefore, if a natural person presents or indicates in the form the type and number of his/her electronically readable document, then he/she can be uniquely identified in the Population Register. In the case of remote identification and authentication through the National Point (Act 250/2017 Coll. on electronic identification), the natural person is uniquely identified by a meaningless directional identifier (BSI), which can be transferred through the information system of the basic registers to the AIFO (service E226).

At local level

Within the information systems of an individual public authority, it is recommended to use the same principles that are used at national level, respecting the fact that this is an agency-specific office where agency-specific data are very likely to be present, and exceptionally data from other agencies.

Accompanying measures

- **Logging -** each access to personal data and their actual linking must be stored in an operational log for at least two years in accordance with the rules of Act 111/2009 Coll.
- **Updating of data -** reference data on a natural person must be kept up to date through the notification system of the basic registers. Agency data from other agencies must be kept up to date according to the rules in force in the agencies providing the data. According to the GDPR, the data processor must ensure that it is working with up-to-date data in order to minimise the risk of an erroneous decision based on outdated data (e.g. sending a decision to an outdated address of a person, or not using the data box of an individual if the person has one). It should be noted here that any public authority that uses certain reference data recorded in the population register in its activities is also entitled to use information on the address to which documents are to be served, the type of data box and the data box identifier, if this data box is accessible (§18(5) of Act 111/2009 Coll. on the Basic Registers).

The above architectural requirements must be implemented at the database and application level so that the users of the information system are not restricted in the performance of the supported agendas. At the same time, the necessary data analysis must determine what data must be kept within the information system. Again, it must be taken into account that although the statutory provision allows for the maintenance of data, this data does not have to be maintained in its value but may be maintained in the form of a reference or other link. The specific decision of the substantive administrator of the agenda must be based on the procedural requirements of the agenda and it is not possible to lay down a blanket unambiguous rule.

An example of this would be the maintenance of addresses within the Czech Republic, where the **recommended practice** is to maintain this data in the form of a reference link to the Register of Territorial Identification (RUIAN) or a local copy of address locations that is kept up-to-date in accordance with RUIAN. This consequently eliminates the erroneous administrative procedure where an invalid address is used.

Another example is the situation where, for example, the date of birth of a person is not used in the agenda for searching or sorting, then this date of birth can be kept in the form of a reference link to the population register and the specific data can be retrieved only when necessary.

Pseudonymisation, AIFO, Identifier, Subject Area