EUROPEAN COMMISSION

Directorate-General for Structural Reform Support

Simplification of the tax reporting obligations for employers in Hungary

REFORM/SC2021/026

Detailed concept of the new reporting system

July 2022

European Commission

PÉNZÜGYMINISZTÉRIUM

Building a better working world

STRATIS GO THE EXTRA MILE

Tartalomjegyzék

Executive summary

Context of the project, characteristics of the current reporting system

Full compliance with employment related reporting requirements requires substantial resources from Hungarian enterprises. Upon engagement by the Ministry of Finance, with funding of the European Commission, a comprehensive survey was conducted on the tax administration costs of businesses in 2019 with 2,000 participating businesses. We may in part conclude—with particular relevance to the present project—that the costs of returns and reporting related to the employer's role are considerably high; in 2018, they amounted to 22 % of total administrative costs (corresponding to HUF 91.87 billion annually, at the level of the national economy).

This level of administrative burden is partly attributable to the fact that the current non-standard (but to a major extent electronically operated) reporting system—applying a periodic approach, adjusted to the operating logic of public authorities and to their deadlines—is inefficient for a number of reasons:

- A number of public authorities require reporting through various systems (and forms), based on different intervals;
- requested data are often very similar and overlapping;
- the role of online data verification is limited in the reporting process, resulting in many avoidable errors identified in the course of official checks (and subsequent manual consultation between public authorities and employers);
- processing databases are operated in isolation, they are typically not connected;
- no meaningful feedback is provided to reporting entities, employees lack basic methods to check data being provided on them.

Chapter 2 contains the comprehensive assessment of the current system.

Based on the foregoing, the Ministry of Finance recognised the need for a paradigm shift to significantly improve the efficiency of the reporting system. Under the financing of the European Union, in cooperation with the Directorate-General for Structural Reform Support, the present project aims to draw up the concept of an event-based, single-channel reporting system capable of replacing the periodic and fragmented approach.

- The initial concept of the new reporting system was drafted in 2021. The current reporting system was assessed as part of this process, followed by conceptual proposals for the new reporting system also in consideration of international best practices, including business process flows and the technological background, and the list of events – replacing the reporting obligation in the future – serving as a basis for the new system.
- In the second phase of the project, the concept is elaborated and detailed; this document is the output of this process. It aims to enable launch of the planning phase of the new reporting system of employers based on the Government's decision, and the business and technological requirements of the planned system.

Characteristics of the future system

Basic features of the future system:

- employer reporting processes are adapted to the operation of employers, also taking into account the needs of public authorities;
- employer data provision is linked to events in place of periodicity;
- employers are required to provide data only on events and changes, but not on unchanged parameters reported earlier, which significantly reduces reporting related redundancies ;
- single-channel reporting is implemented, i.e data are provided once, in a single form to a central system, from which public organisations can directly access the data relevant to them, considerably reducing the volume of data reporting obligations for employers, as certain data (e.g. sickness data for social security institutions) and data provisions (e.g. statistical data) will no longer be required under the new system);
- State actors would also report relevant information, authentic data currently managed on paper and/or unavailable online to the central system;
- employees can share authentic data with their employers and track reported data concerning them.

To achieve these goals, the new reporting system will provide the following key functions and services:

- **Simplified identification** – in contrast to the current system, data providers will have fewer identifiers to manage thanks to the support of the relevant specialised system.
- **Complex checks prior to data submission** – prior to data submission, complex checks will be carried out, backed up by a comparison of the data from public administration IT systems, previously submitted events and payment events to be submitted together. Complex checks will significantly improve the quality of the data sent to public authorities, thereby substantially reducing the number of incorrect data submissions and the administrative burden on both public authorities and employers due to manual corrections of errors afterwards.
- **Data provision forms transformation** – based on the built-in functionality of the data reporting system, public authorities can continue to use the current data provision forms, albeit on a temporary basis, while employers can become independent of the data provision forms.
- **Use of data from public administration IT system** – in addition to eligibility checks, the data reporting system will channel in data already available in the public administration IT systems, so that employers do not have to report them again. This reduces the burden on employers and contributes to the principle of data minimalisation, as reporting agents have fewer personal data to process.

Chapter 3 describes the detailed concept of the future system, while Chapter 5 sets out the functional and non-functional requirements of the system. Chapter 8.2 also describes the operation of the reporting system in practice through a case study.

Design of the proposed IT architecture

The new reporting system is based on the premise that most employers already record event data elements in their payroll systems; in their case, the method of data recording will remain the same, while reporting will be performed through the payroll system in an integrated manner. For companies not operating a payroll system (or outsourcing payroll accounting), the new system offers a web platform and mobile application for meeting the reporting obligation.

The proposed IT architecture is built on the event-based reporting platform (EMAP), which establishes a connection between employers, employees and public bodies ensuring the event-based performance of mandatory reporting related to employment. It also enables employees to share their data with employers, and, in the function of an authentic storage provider, it supports access to provided event data for authorised parties.

The system performs formal and substantive verification of employment data submitted by employers, stores and transforms such authentic data to a format read by official specialist IT systems (e.g. NTCA (National Tax and Customs Administration), NHIF (National Health Insurance Fund of Hungary), HCSO (Hungarian Central Statistical Office), HST (Hungarian State Treasury)), until these can receive native event data. The system architecturally builds on already established government electronic services (e.g. KEÜSZ/SZEÜSZ (Central Electronic Administration Services / Regulated Electronic Administration Services)) and information provided by administrative specialist IT systems and other public reporting systems.

The main software elements of the future system are as follows:

- **Employer data provision systems**: payroll systems prepared for automatic data provision or browser-based web and mobile applications;
- **EMAP – Event-based Reporting Platform:** the newly implemented central system that receives data provision from various parties and makes relevant event data available to data processing organizations (authorities);
- **State reporting systems:** existing public administration IT systems that send data on specific events to the EMAP based on laws or the employee's authorisation and make these accessible to employers and other authorised public bodies;
- **State data processing systems:** existing public administration IT systems receiving and processing data from the EMAP, reported by the employer, returning authentic employee data to the EMAP, and performing additional administrative tasks.

In the framework of the project, two possible technological solutions for the implementation of the new system were examined: 1) a private (closed, permission-based) distributed ledger technology (DLT) based on a "proof of authority" consensus mechanism and 2) a solution based on centralized data processing and storage (KAF). The main advantages and disadvantages of these two solutions are as follows:

- DLT benefits: it offers preventive security solutions of outstanding quality, the technology guarantees authenticity of reporting and its distribution in nodes operated by authorities by virtue of its integrated features.
- DLT disadvantages: being a new technology, the method still needs to mature, there are no standards yet, there is uncertainty regarding scalability and transaction processing speed, and its storage capacity requirement is also larger than of the other technological solution.
- KAF benefits: mature architecture and technological solutions are available, the implementation and operational risks can be well assessed, in parallel with available professional competence. The system enables good scalability by use of cloud-based technologies and micro-services.

- KAF disadvantages: Data integrity is ensured by the quality of development and operation, breaches are investigated by detective work, no independent guarantees for reporting authenticity.

The new system is realistically feasible with both technologies; the two solutions are comparable for development costs. In terms of data storage, in the case of DLT, a larger data storage capacity requirement shall be expected if event data is stored in a blockchain.

The means of managing data protection rules is key to the feasibility of the event-based reporting concept. Due to single-channel reporting, all data sets are physically stored in one database in relation to both technological versions, in terms of data protection legislation it is necessary to examine whether data encryption and authorisation management provides sufficient protection to ensure that only designated controllers can access given data sets.

Based on the analysis of the technological advantages and disadvantages of DLT, we proposed a hybrid architecture version, which combines the advantages of the two technological solutions while trying to eliminate their disadvantages. The basic essence of the model is that, while the event data related to natural persons and employers are stored in a centralized database with the technology offered by KAF (with encryption and strong access protection solutions), the validated hash codes formed from event data would be stored separately in blockchains (using the DL technology).

Supplementing the solution using purely KAF technology with the DLT increases the complexity of the project, but it provides the additional feature that the authenticity of the data provision is independently ensured and can always be verified due to the internal nature of the technology.

Chapter 4.2 describes the proposed IT architecture .

Key findings relating to the system's introduction

The system can be implemented, but its introduction demands substantial efforts from all stakeholders involved. We draw attention below to key aspects:

- The introduction of a new system in a single phase is not realistic in relation to the present project, as the volume of development and the degree of change carries significant risk. There are a number of possible solutions for phased introduction; moreover, phasing can be supplemented with various concessions, services (grace period, voluntary connection in the initial period, support of reporting entities with cheap software solutions). We propose the implementation of a pilot phase, in which – with the involvement of maximum ten companies, joining voluntarily – the core functionalities of the new system can be tested, identifying in a cost efficient manner any potential flaws in due time.
- According to expert estimates, preparations for the new reporting system require three years; the pilot system could be launched from the send half of the 3rd year, if certain conditions are met (clear support by senior management, flexibly cooperating stakeholders, and efficient project management).
- We estimate the cost of development, introduction, and support to be close to 30 billion Hungarian forints. This does not include the cost of public administration IT system development essential at subsequent stages (the amount of which can be determined on the basis of a separate assessment).
- The reform will offer quantifiable benefits in terms of administrative burden for employers, with an average reduction of 42.6 percent of time needed for companies to provide employment data at the national level. This represents a financial saving of HUF 20 billion per year and at the level of the national economy, which means that the estimated payback period for the total

development costs is less than 18 months (excluding the cost of the system improvements required by the authorities).

- The preparation, implementation and operation of the envisaged new data provision system pose significant professional management and administrative coordination challenges. Given that the project will require the active involvement of a number of governmental organisations, the establishment of an inter-ministerial consortium management structure and the appointment of a dedicated government commissioner are necessary to ensure the successful implementation of the reform. The consortium should include representatives from the Ministry of Finance, NTCA, HCSO, HST, NHIF, Ministry of Interior, Digital Hungary Agency Zrt. and any other data hosting organisations.

The details of the implementation plan (including the work packages) are presented in Chapter 6, and the costs of implementation and quantifiable savings are presented in Chapter 7.

1. Context and purpose of the project

Full compliance with employment related reporting requirements requires substantial resources from Hungarian enterprises. Upon engagement by the Ministry of Finance, with support from the European Commission, a comprehensive survey was conducted in 2019 on the tax administration costs of enterprises with the participation of 2,000 enterprises. It was aimed at providing a representative view of the amount and structure of tax administration costs.[1]

At national economic level, the tax administration costs of enterprises in 2018 amounted to HUF 420 billion, equalling 1.7 percent of their annual revenue. The research found that time spent with tax administration proportionately increases with enterprise size, but the specific time (per one employee) is significantly higher for smaller employers. Moreover, the time required for reporting related to the employer's role is by far the highest compared to other types of tax (corporation tax, value-added tax).

The research also established—with particular relevance to the present project—that the costs of submissions and data provision related to the employer's role are considerably high; in 2018, they amounted to 22% of total administrative costs (corresponding to HUF 91.87 billion annually, at the national economic level).

This level of administrative burden is partly attributable to the fact that the current reporting system related to taxation is inefficient:

- First, it demands substantial resources on the part of both Hungarian enterprises and (in terms of control and processing) public authorities.
- Second, the non-standard system shows significant overlapping. Within the current reporting system—based on a periodic approach, adapted to the operating logic of public authorities—a number of public authorities often collect the same data through various systems (and forms), at different intervals, while the processing databases operate in isolation and are typically not connected. This imposes significant burdens on the employer side in terms of both operation and development.

The Ministry for National Economy carried out an analysis as early as 2017, which reviewed the feasibility of options for simplification relating to employers' reporting to reduce redundant reporting (and hence administrative burdens). The analysis extended to shortening forms, reducing their frequency, the direct reduction of the administrative burden, the uniformisation of forms and reporting serving similar purposes, and to the integration of statistics gathering. Specific development projects were ultimately not launched on the basis of the proposals put forward mainly because based on feedback provided by market operators and experts involved in consultations, the proposals would not have led to substantial progress proportionate to the costs of reforming the system. The logic of the proposals, however, underlined the necessity of a paradigm shift in several respects (uniformisation and replacement of forms, offering of data processed by the State).

The Ministry of Finance confirmed this in its presentation held at the Tax Conference of the National Tax and Customs Administration in November 2020. After presenting the current tax administration environment, the presentation also put forward proposed solutions in the decision-making phase, aimed

[1] The study conducted by EY and Budapest Institute is available at:
DG REFORM_HU_Compliance_cost_report_200618.pdf (kormany.hu)

at a new, event-based approach to reporting. The Ministry of Finance thereby clearly indicated that comprehensive structural reform, a paradigm shift is needed for a substantial improvement in efficiency.

The aim of the project is to develop a reporting system that will be characterised by:

- Where possible, the system will cover the full range of employment-related reporting (the exact range of forms covered by the project is set out in Chapter 2.1).).
- Employer reporting processes are adapted to the operation of employers, also taking into account the needs of public authorities.
- The periodic approach is replaced by event-based reporting, thereby eliminating the obligation to provide data not containing any new, meaningful information.
- The current fragmented system is replaced by single-channel reporting, data are provided in a unified form and channel to a central system, from where public authorities can produce their own necessary statements.
- Public authorities would also record relevant information within the central system.
- Employers and employees can also access event data relating to them.

In 2021, the first conceptual design of the new data system has been completed. As part of this, the current reporting system was assessed, and conceptual proposals for the new reporting system were developed, taking into account international best practices, including business processes and technological background, as well as a list of events that will trigger the reporting obligation in the future, on which the new system will be based

In the second phase of the project, the concept will be deepened and elaborated in more detail, and this document is the product of this work. The aim is to start the design phase of the new employment data system, based on the business and technological requirements of the planned system, subject to the decision of the Government.

The project was financed by the European Union through the technical support instrument, in cooperation with the Directorate-General for Structural Reform Support of the European Commission..

This document is structured as follows:

- Chapter 2 presents and assesses the current data reporting system, indicating how the new logic can provide a meaningful response to key challenges.
- Chapter 3 presents the business requirements for the new system and a description of the operating model of the new system;
- Chapter 4 details the recommended IT architecture of the system, including the comparative evaluation of the two technological solutions examined.;
- Chapter 5 elaborates the functional and non-functional specification using the requirements identified;
- Chapter 6 presents the development and implementation plan of the new system, including the timetable and the recommended work packages of the development process;
- Chapter 7 quantifies the benefits of the introduction of the new system;
- Chapter 8 includes the document's annexes (referred to in the document).

2. Presentation and evaluation of the current reporting system

2.1. The nature of data reporting

Employers' reporting to public authorities in Hungary is currently organised along the lines of periodic, form-based logic. It is adapted to the method of public authorities (public authorities) processing data provided by employers in terms of both timing and structure. Employers typically provide data on a periodic basis (annually, quarterly, monthly, daily) by completion of forms provided by public authorities. The forms are units of reporting, which in themselves have to be meaningful with due completeness for public authorities. The project covers four public authorities (National Tax and Customs Administration, Central Statistical Office, National Health Insurance Fund Management Office, Hungarian State Treasury), which provide employment data, summarised by type and frequency in the table below. The data reporting reform will cover all citizens with an employment relationship (including self-employed persons).

Data provision form	Relevant authority/Participant	Responsible for data provision	Frequency / deadline
2108	National Tax and Customs Administration (NTCA)	Employer, paying agent	Monthly / until the 12th day of the following month
2158	National Tax and Customs Administration (NTCA)	Self employed persons, primary producers	Monthly / until the 12th day of the following month Quarterly (primary producers)
2108INT	NTCA	Foreign employer	Monthly / until the 12th day of the following month
T1041	NTCA	Employer, who employs the insured person	event-based
T1042E	NTCA	Employer, who employs simplified employee	event-based
T1041INT	NTCA	Foreign employer who is not registered in Hungary, but who employs the insured person	event-based
T1044D	NTCA	Employer, who employs school cooperative members	event-based

Data provision form	Relevant authority/Participant	Responsible for data provision	Frequency / deadline
TMUNK	NTCA	Employer, who employs temporary workers	event-based
MÁT I- Additional leave statement summary form for the father	Hungarian State Treasury (HST)	Employer	quarterly / until the 31st of March, the 30th of June, the 30th of September, and the 31st of December
OSAP no. 1117 – Workforce expense	Hungarian Central Statistical Office (HCSO)	Employer	annually / until the 31st of May of the following year
OSAP no. 1405 – Individual wages and earnings	HCSO	Employer	annually / until the 15th of March of the following year
OSAP no. 2009 – Quarterly employment report	HCSO	Employer	quarterly / until the 12th day of the following quarter
OSAP no.2241 – Annual employment report	HCSO	Employer	annually / until the 1st of March of the following year
E-Jelent – in case of passive care	National Health Insurance Fund (NHIF)	Social security disburser	Announcement of passive care is event-based
EB-21	HST	Social security disburser	monthly / until the 12th day of the following month
OSAP no. 1514. Monthly Health Insurance Statistical Report	HST	Social security disburser	monthly / until the 11th day of the following month
OSAP no. 2395. Report of closed incapacitated for work cases	HST	Social security disburser	quarterly / until the 11th day of the following quarter
OSAP no. 2396. Report on baby care benefit recipients	HST	Social security disburser	quarterly / until the 11th day of the following quarter
OSAP no. 1914. Report on recipients of childcare benefit and adoption benefit	HST	Social security disburser	quarterly / until the 11th day of the following quarter[2]

[2] Parallel to the implementation of the e-PELL project, the EB-21 Paying Agency accounting and the 4 OSAP data reporting services, which are the responsibility of the Hungarian State Treasury, will be discontinued in this form. The social security payment offices will provide a single - individual, social security number based - data reporting to the health insurance company on a monthly basis. The e-PELL system is currently planned to operationalize on 1 July 2023; the related legislative proposals will be submitted to the legislator in the Autumn 2022 legislative cycle.

Data provision form	Relevant authority/Participant	Responsible for data provision	Frequency / deadline
K36 ('108) - MRP organization	NTCA	Employer	annually/ until the 31st of January of the following year
K91 simplified tax (Ekho)	NTCA	Employer	annually / until the 31st of January of the following year
Tax allowances	Employer	Employee	event based
Special data provision for civil servants, public servants, non-profit organizations and school associations	NTCA, HCSO, NHIF	Organizations, associations Organizations and associations do not have reporting obligation toward NHIF	annually, quarterly, monthly
Rehabilitation contribution – Form 01	NTCA	Employer, paying agent	*quarterly / until the 20th day of the month after the quarter, the difference by 25th day of February after the actual tax year*

Table 1: Employer data provisions covered by the project

In addition to the data provided by employers, there are also a number of data transfers between different authorities.

Frequency of reporting	Presentation of the types of reporting
Monthly	▶ The NTCA provides data each month on a specific set of contribution data to the following public authorities: HST, NISP (National Infocommunication Service Provider), HCSO, NHIFA, Prime Minister's Office, Ministry of Human Capacities, Educational Authority, Ministry of Technology and Industry, Ministry of Finance. ▶ Within the HST–HCSO relationship: labour data of budgetary public authorities within the KIRA system
Quarterly	▶ Within the NTCA–NHIF relationship: reporting related to deceased taxpayers
Annually	▶ Within the NTCA–HST relationship: Base and amount pension contribution declared in the PIT form
Daily	▶ Within the NTCA–HST relationship: data relating to social contribution tax benefits ▶ Within the NTCA–NHIFA relationship: Multiple daily transfer of reports T1041, T1042

Table 2: Data provision between authorities relevant to the project

2.2. Process of the data provision

Due to the predominantly periodic arrangement of the current reporting system, reporting entities meet obligations from time to time through the process below, adjusted to reporting frequency:

Figure 1: The reporting process

We present below our findings relating to specific process steps.

Collection of data sets relating to reporting

In this function group, the dominant administrative burden is posed by the second process step, the collection and recording of supporting documents and data supporting events.

- At larger companies, most data are received electronically. This may involve both reporting through an automatic interface and manually imported Excel tables, if an appropriate interface is unavailable.
- The two most critical areas involve dataf related to sick pay and sets of data on presence. In the case of the former, the main burden stems from the obligation to collect data on paper; in the latter case it stems from the precise recording of data and possible corrections. Additionally, based on the findings of interviews conducted during the project, employers reported the major administrative burden of various employee declarations at the beginning of the year, such as the declaration on supplementary leave.[3]
- A mixed reporting system is operated on the field of tax benefits: persons without Client Gateway access are required to issue declarations on paper to their employer. Employees with Client Gateway access can issue the declarations to NTCA through ONYA and then the declaration will be forwarded to their employer (although many still choose paper-based administration).

Data verification

- Three levels of verification are essentially distinguished in relation to employers' reporting. This function group contains the first level, where the conformity of collected data is verified by the employer and payroll provider.
- Based on general feedback, verification and cleaning of data consumes a lot of time. This is necessary less in relation to staff data, but more in relation to labour data. Verification of data relating to health care is very labour intensive for employers. Currently, namely, employers are required to collect the vast majority of such data on paper, the interpretation and verification of which requires substantial manual labour. An interviewee providing payroll services also noted that health care documents often also contain personal data employers/payroll providers do not need in the given case.
- Some payroll software performs automatic formal verification in relation to standard form-based reports. Payroll providers typically directly consult with clients if they detect incorrect data .

Preparation of data necessary for reporting

- While major software can produce data necessary for forms, more simple software solutions often used by small enterprises have limited functions, hence users have to manually perform certain tasks.
- Quarterly reporting to the HCSO is most labour intensive in terms of data preparation, as payroll software provides such data not through an interface, but in pdf format, which is manually uploaded by payroll to the Elektra system.
- When reporting to the HCSO, for example, it is often a problem for employers to complete the data request questionnaires based on basic statistical terms. They often don't understand these and often request position papers from the HCSO.

[3] Currently, due to legal obligations, this must be completed on paper .

Data provision

Employers are required to provide data on different forms to a number of public authorities, often involving identical or similar data content, but with different timing.

Reporting to the NTCA:

- The General Form Completion Programme (ÁNYK) and its web version, the Online Form Completion Application (ONYA) available since 2019, are some of the main channels for filing submissions and reporting to the NTCA. Only certain forms can be submitted through the latter for the time being (currently around 20 forms), but their number is continuously increasing on a scheduled basis. Since the user logs in to the ONYA platform through identification, registered master data are quickly matched with the reporting entity.
- As regards the usability of the ÁNYK, however, stakeholders put forward criticism: The system allows submission of outdated forms (only subsequently indicating the error); the related receipts are not sufficiently clear or user-friendly; its use overall consumes unreasonable amount of time. The system performs pre-reporting verification (verification of data entered on the electronic form) but is unable to support online verification of data stored in public administration IT systems.

Other reporting:

- Employers are required to upload data to the HCSO within its own system (ELEKTRA).
    - As a frequent problem, employers are required to provide data along the lines of unclear terms. The relevant terms are defined not at legislative level, but various completion guides contain examples. Interpretation of the precise data requirement is therefore very time-consuming.
    - Within the ELEKTRA system it is possible for employers to check, possibly correct and send data sets uploaded by the payroll provider. In relation to the this, it is problematic that often large quantities of data sets need to be uploaded, where it is not possible to correct specific data after the upload, only by uploading the entire data set again.
- A problem in reporting to the HST is the lack of implemented data validation.[4] Interviewees agree that they are burdened with a significant amount of redundant data provision in relation to the HST (eg. GYÁP declarations).
- Reporting is performed by post, on e-Paper or through e-Reporting to the NHIFA. The NHIFA, however, receives data within its competence through the NTCA.
- Interviewees also noted the positive example of the ease of use of mobile apps supporting simplified employment and online invoicing.

The second step of three-step verification of reporting to public authorities is performed by use of applications used for reporting (e.g. ÁNYK, ONYA, Elektra), where applications perform formal verification of entered data.

[4] The problem will already be remedied within the framework of e-PELL. e-PELL is the development project of the HST, where an IT system is developed for data processing relating to the accounting of cash benefits and accident sick pay. The development aims to reduce administrative burdens and improve the quality and transparency of service through reduced manual procedures. The system would also process information received from the NTCA and support the return of related decisions.

Processing of provided data

As part of data processing, significant amounts of data are exchanged between public authorities in accordance with contract terms applicable to them.

- Among the public authorities, the NTCA forwards data to the most partner bodies. The NTCA forwards significant data quantities to the NHIFA: 90 percent of data received by the NHIFA is sent by the NTCA through asynchronous machine-to-machine technology. If the NHIFA detects an error in data received from the NTCA, it provides feedback, but the NTCA is responsible for managing the error. The NTCA forwards the following forms to the NHIFA:
    - T1041, T1041INT, T1042E (with immediate online delivery));
    - Data parts from 08, 08INT, 058 returns monthly, backdated by two months.
- The HST provides data to the HCSO in relation to OSAP reporting . First, it consolidates from social security payment offices and government offices and provides it to the HCSO in OSAP format. The HST forwards the following forms to the HCSO:
    - OSAP 1514 - Monthly Health Insurance Statistical Report,
    - OSAP 1914 - Report on persons receiving childcare benefit and adoption benefit,
    - OSAP 2395 - Report on closed cases relating to incapacity for work,
    - OSAP 2396 - Report on persons receiving infant care allowance.
- The NTCA also forwards a number of other data to various public authorities, where specific data content of forms is provided at various intervals. Some examples of the above:
    - To the HST, monthly: aggregate contribution data for employed persons in receipt of an early retirement benefit or a service pension in excess of or below the annual reference amount of the income on which the social security contribution is based;
    - To the Ministry for Technology and Industry, quarterly: Data on the amount of healthcare service contribution differences among monthly tax and contribution forms submitted by social co-operatives;
    - To the HCSO, monthly: Staff size data of VAT payers.

Based on interviews conducted with representatives of relevant public authorities, data processing is encumbered by the following challenges:

- The retroactive correction of data was identified as a common problem for public authorities in relation to correction requests. Employers often provide data late, which may also cause major errors, difficulties in processing due to retroactive modifications. Late receipt of data also results in additional work for employers.
- Certain data are still recorded manually, involving substantial human labour. Human labour cannot be omitted when managing blocked items, for example, as administrative decisions based on complex rules are required. This imposes additional burdens mainly on data providers.
- Possible differences in data exchange between NTCA and NHIFA are caused by the different approaches of the two organisations (NTCA: self-taxation principle and NHIFA: legal basis). Nevertheless, a significant number of errors are caused by incorrect completion of forms (mixing up tax identification number and social security number, incorrect entry of employer's data). Several interviewees confirmed that in some cases, data in the NHIFA and NTCA records may vary (e.g. FEOR (Standard Classification System of Occupations) number). In relation to the above,

payroll providers are of the view that it should be possible for employers to retrieve data related to them in official records, thereby ensuring validation of such data.[5]

The third step of verification of reporting to public authorities is performed after receipt of forms. Based on NTCA statistics for the years 2020 and 2021, 3–10% of originally submitted forms are incorrect, which is well over one million originally incorrect forms in 2020. These forms were cleared in the first step of data verification; the ÁNYK and ONYA qualified them as fit for submission. An analysis of NTCA identified the following common recurring errors in tax returns:

- In forms containing numerical data, significant differences resulting from obligations stated in HUF instead tHUF (e.g. company car tax));
- self-review error attributable to the taxpayer incorrectly calculating the detected difference compared to the preceding form;
- problems related to incorrect designation of the submission period, e.g. incorrect starting or closing date, or data not matching data stated in the T1041 form of the insured;
- use of incorrect master data relating to employees (e.g. date of birth or tax identification number), which results in variation from identification data contained in the NTCA records;
- the given legal relationship cannot be identified in relation to reported legal relationships based on the stated start and code of the legal relationship;
- the employer reports data on the TMUNK form, which it had already reported.

Where incorrect data are provided, the public authority requests corrected reporting.

[5] On the part of NHIFA, the external reporting type of data is already available electronically in xml format, which can be used by filers, payroll processors.

2.3. The relevant data sets

Currently employers are required to fill in a total of 1899 data fields on the 23 forms covered by the reform; 889 of these are substantive data fields, while the rest serve as identification (further elaborated in Chapter 8.2). The covered data fields can be classified into the following sets: :

- **Identification data:** Each of the forms—irrespective of their basic purpose—contain identification data to ensure that public authorities can clearly match received reporting with the given employer or employee (tax number, tax ID, social security number, name, address, etc.). Such data make up around 48 percent of data fields.
- **Data relating to employment:** Basic data classifying the employee (e.g. type of insurance, start and end of insurance, FEOR number, work schedule); some of these don't necessarily change often, employers are nevertheless required to report them on a monthly, quarterly, and annual basis on various forms. Such data make up around 8 percent of data fields.
- **Wage data:** Data provided mainly in relation to wage payments (there are forms, however, also requiring reporting of contractual wages) with a breakdown and focus of varying detail. A wide range of forms relies on wage data, whether in a monthly breakdown (e.g. 08) or at less frequent intervals (e.g. the OSAP 2009 Quarterly Labour Report each quarter, OSAP 1405 Reporting of Individual Wages and Salaries each year, OSAP 1117 Labour Cost Reporting). Such data make up around 5 percent of data fields.[6]
- **Data relating to the tax and contribution base:** With regard to the above, the 08 form is the most comprehensive one submitted each month for individual employees (serving declaration of taxes, contributions and vocational training contribution relating to payments and benefits), with other forms also covering similar data (e.g. the 08INT and 58 form relating to a special scope of data, such as self-employed persons not deemed to carry out ancillary activity and insured primary agricultural producers). Such data make up around 17 percent of data fields.
- **Data relating to incapacity for work:** Data relating to sick pay (including accident and child nursing sick pay) and other incapacity for work are recorded on several forms (EB21, OSAP 1514 Monthly Health Insurance Statistical Report, OSAP 2395 – Report on closed cases relating to incapacity for work, Data sheet for proof of continuous incapacity for work, Employer's certificate). Such data make up around 7 percent of data fields.[7]
- **Rehabilitation data:** The rehabilitation contribution is primarily reported on the NTCA 01 form, but the item is also stated in the 08 form and on the OSAP 1117 form. Such data account for less than 1 percent of data fields.
- **Statistical data:** The forms of the HCSO (e.g. OSAP 2241 Annual labour report, OSAP 1405 Reporting of individual wages and salaries) regularly include statistical terms (e.g. average statistical number of employees, salary, presence data), which by their logic are difficult to match with forms submitted to the NTCA in relation to similar topics. Such data make up around 15 percent of data fields.

[6] There is significant overlapping between the category and statistical data. Data fields possibly falling into both categories are classified among statistical data. Similarly, there is also overlapping related to the tax and contribution base; these data fields are classified among data related to the tax and contribution base.

[7] There is also significant overlapping between the category and statistical data. Data fields possibly falling into both categories are classified among statistical data.

Data obtained from data reporting required by individual public authorities and through the exchange of data between public authorities will be stored in different official registers. Pursuant to Section 36 (2) of Act CL of 2016 on General Public Administration Procedures “the client shall not be required to attach a professional opinion or a preliminary professional opinion and, with the exception of information necessary to identify the client, information which is public or which must be contained in an authentic register established by law." Although public authorities strive to comply with the cited legal requirement, in practice this is not the case. At present, in terms of the following data sets, employed individuals and employers provide data that are potentially available in state and official registers:

Related data sets	Related official database	Public authority / government organisation concerned
Records of reduced capacity to work	Electronic Rehabilitation Management System (e-RSZR)	Hungarian State Treasury
Register of personal and address details	Personal data and address register (SZL)	Ministry of Interior
Registry of birth certificates	Electronic Certificates (EAK)	Ministry of Interior
Records of employment-related data	Integrated System	Ministry for Technology and Industry
Records of data related to social benefits	System of benefits in cash and in kind	Ministry of Interior
Records of pensions and retirement benefits	NYUFUR (Pension payment) system	Ministry of Finance
Health insurance records	BSZJ - Register of insurance status of declared persons	NHIF

Table 3: Data sets available in the state register

Furthermore, we understand that the integration of disability data into EESZT is under preparation. Its implementation would greatly simplify the data reporting process.

2.4. IT background of the current system

In each data reporting segment, public authorities have access to some form of electronic support in the case of their data reporting concerning employment. At the same time, the technological background of administrative support is highly heterogeneous in terms of quality and scope, both in the case of employers (data providers) and state and private organizations (data processors) that process employers' data reports.

Below is a schematic diagram of the actors involved in the reporting, the types of systems and the relationships between them:

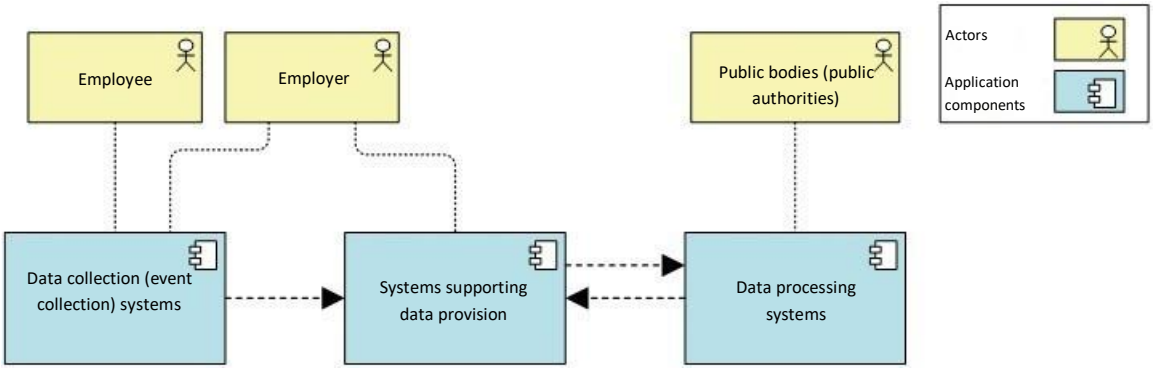

Figure 2: Conceptual architecture of IT applications that ensure employers' data reporting

The following table shows the roles and main tasks of the types of applications involved in fulfilling employers' data reporting.

Types of information systems	Description
Data collection (event collection) systems	Registries collecting and managing the underlying data sources of reporting, and the registries producing the files necessary for the reporting, such as ▶ Personnel management systems (HR systems), ▶ Payroll systems and ▶ Other employment data management systems (e.g., access control, work time and attendance systems, leave records). It is also typical for the data collection systems used by employers that electronic business support systems are supplemented with manual data recording and paper-based records. The degree to which the data collection process is automated and IT-supported, and - in this context - the quality of the data, depends on the level of digitisation of the company.
Systems supporting data provision	To support the data provision of employers, public authorities have various purpose-built systems supporting data provision (e.g. ÁNYK, ONYA), the main functions of which are: ▶ Recording and importing data;

Types of information systems	Description
	▶ Formal and internal logical verification of data; ▶ Submission of data; ▶ Acknowledgment of data submission. Systems supporting data provision include general purpose systems (e.g., e-Paper) and non-digital options (paper). A significant amount of data transmission and inter-public authority reporting take place between public authorities using the data collected from the employers' data provisions. The technological solutions of the data provision tools are heterogeneous, both older (mass data transfers on MQ channel and DVD, individual data transfers with the help of individual data queries recommended by KKSZB) and new, modern technological solutions are available, however, the data provider must adapt to the available technological possibilities and the required reporting formats.
Data processing systems	Data processing systems operated by public authorities receive and process the data provided by employers. Main features relevant to the provision of data: ▶ Receipt and confirmation of data provision; ▶ Verification of reported data; ▶ Producing data reports for other public authority; ▶ Fulfilling the data requirements of employers.

Table 4: IT application types

The diagram below shows the connections (interfaces) between the IT systems involved in the employers' data provision.

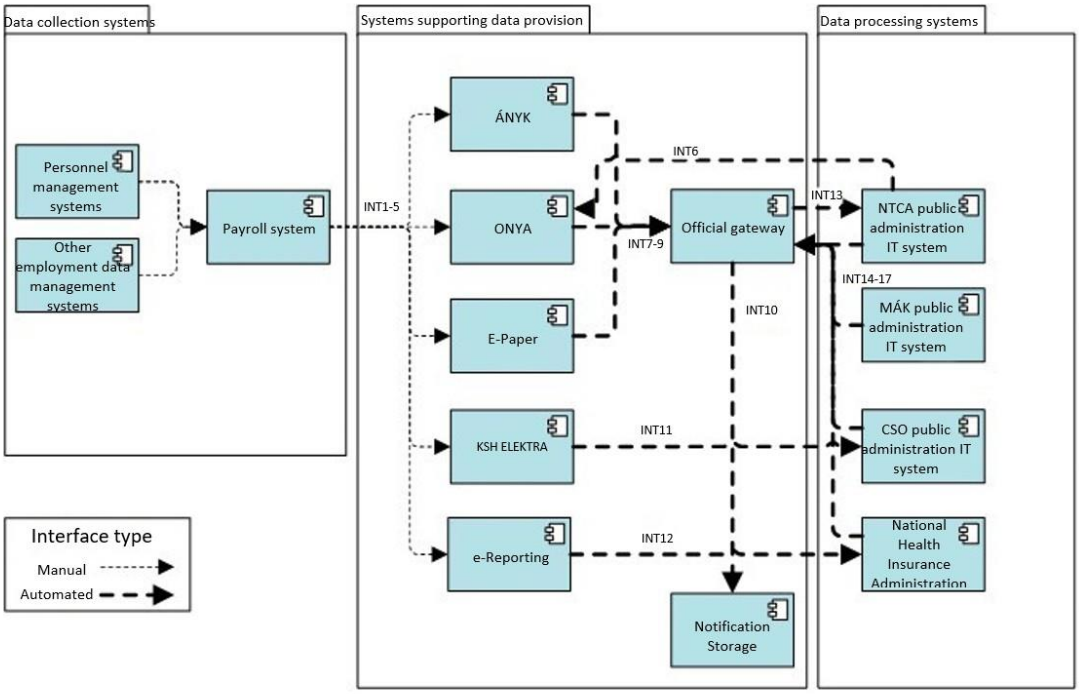

Figure 3: Application architecture for employers' data provision

2.5. The infrastructural background of the current system

For the electronic support of data provision, the affected applications use the central and regulated electronic services provided by the state (SZEÜSZ/KEUSZ).

Információs rendszer	Leírás
Secure Delivery Service (BKSZ)	BKSZ is a service that ensures the delivery of electronic messages in accordance with the specified technical specifications, to which the storage facility for official electronic communication and the secure delivery service address service are closely related: ▶ Official Gateway for public authorities providing electronic administration ▶ Company Gateway for economic entities and ▶ Client Gateway for individuals.
Company Gateway (CK)	The Company Gateway is an electronic repository for business organisations, where all concerned and authorized persons can access the official correspondence of a given company or organisation in one place.
Central Identification Agent service (KAÜ)	The Central Identification Agent (KAÜ) is a comprehensive identification service that carries out identification within regulated electronic administration services and forwards it to users and institutions.
Client Gateway (ÜK)	An electronic client access and identification system that allows the user to communicate securely with organisations providing e-government administration and e-government services. The service is used by customers who use electronic administration.
Official gateway (HK)	An electronic service that allows organisations to receive authenticated electronic messages, and the electronic messages of offices to be delivered to authenticated clients (citizens, offices, economic entities).

Table 5: Central and regulated electronic services

2.6. Evaluation of the current system

Hungarian enterprises need to possess substantial resources to ensure full compliance with employment related reporting requirements. Upon engagement by the Ministry of Finance, with support from the European Commission, a survey was conducted in 2019 on the tax administration costs of enterprises with the participation of 2,000 enterprises.

We may in part conclude—with particular relevance to the present project—that the costs of submissions and data provision related to the employer's role are considerably high; in 2018, they amounted to 22% of total administrative costs (corresponding to HUF 91.87 billion annually, at the level of the national economy).[8]

This level of administrative burden is partly attributable to the fact that the current non-standard (but to a major extent electronically operated) reporting system—applying a periodic approach, adjusted to the operating logic of public authorities and to their deadlines—is inefficient for a number of reasons. A number of public authorities often collect the same data through various systems (and forms), at different intervals, while the processing databases operate in isolation and are typically not connected. This imposes significant burdens on the employer side in terms of both operation and development .

After separately assessing the suboptimal elements of the system, we are presenting the findings of the current system's evaluation as a conclusion below: :

- **Form based reporting logic:** The reporting logic is adapted not to the processes (economic events) of enterprises, but to the operating logic of public administration.
- **Very similar and partly overlapping information needs:** Within the current form-based data provision system, often very similar data must be sent to different public authorities (in some cases the same data in a different breakdown). There is significant redundancy on the level of the data: 70% of data are included on two forms and 70% of data content is sent to at least two public authorities on various forms.
- **Use of different terms:** The standardisation of the reporting system and elimination of the requirement of overlapping information is significantly impeded by certain public authorities' use of different terms in some cases in relation to reporting of economic events. Around one quarter of data fields within the current reporting system (not serving identification) require some form of conceptual consolidation for future single-channel reporting. This is mainly the case in reporting to the NTCA and HCSO; the conformity of contribution forms with statistical terms, namely, is limited, currently justifying separate data collection. This is also problematic for employers: based on feedback, quarterly reporting to the HCSO is most labour intensive in terms of data preparation, as such data cannot be automatically produced from payroll data, and often employers are unable to clearly interpret statistical concepts (e.g. average statistical number of employees, salary, presence data).
- **Requirement of providing data available in public databases:** According to the principle stipulated by law, the State may not request data from reporting entities that are already available in a database. Although public authorities aim to comply with this rule, it is often not enforced in practice. For example, data on reduced capacity for work are registered in the Electronic Administrative System for Rehabilitation (e-RSZR), and personal and address data are registered in the Personal Data and Address Registry (SZL).

[8] EY-BI (2019), 37-40. oldal

- **Reporting with different timing:** There is already event-based reporting (the most prominent example being the submission of basic data on current employment through the T1041 form), but the periodic approach remains dominant. Most forms are submitted each month (but may have different deadlines, as the case may be), while some reporting is performed on a quarterly and annual basis. The complex reporting system, requiring continuous monitoring, imposes a substantial administrative burden on employers, as indicated by the fact that 39% and 13% of companies outsource employment related administration, including reporting, entirely and partly, respectively.[9]
- **High rate of incorrect reporting:** Based on NTCA statistics for the years 2020 and 2021, 3–10% of submitted forms are incorrect, which is well over one million originally incorrect forms in 2020; these were detected by the NTCA internal control mechanisms. Their processing and correction imposes a substantial administrative burden on the NTCA and employers (and similarly on other public authorities in relation to their own reporting).
- **Only limited functioning of online validation:** There is a low number of online checks of data registered within the relevant public administration IT system during the entry and prior to sending of data. Most errors identified during data processing could be avoided if the official data processing systems would send an error message to data providers on incorrect data prior to data submission.
- **Varying level of digitisation in the reporting process:** The vast majority of reporting forms can now be accessed and submitted electronically, which, however, may necessitate manual data input in several cases (uploading of Excel tables on an online platform). Paper-based reporting obligations continue to exist, for data relating to cash health insurance benefits, for example, obviously, the largest administrative burden is related to these.
- **Varying level of digitisation at employers:** IT support for the collection of data necessary for reporting and the IT maturity of the data collection systems shows a very diverse picture. The level digitisation is typically lower at smaller companies, resulting in higher specific labour intensity for data collection, processing of unstructured data, data cleaning and collection of missing data.
- **Outdated reporting systems:** The public authorities provided useful applications to employers, most of which, however, have become outdated. First, they use outdated technologies with inherent security risks (Java Runtime Environment), and second, they cannot be integrated with data collection systems, and data are provided manually (e.g. uploading of xml files).
- **Wide range of secondary reporting:** In line with legal authorisation, certain reporting is delivered not directly to the relevant public authorities, but through partner public authorities. Mainly the NTCA (forwarding to the NHIFA and HCSO) and to a lesser extent the HST (forwarding to the HCSO) are forced into a "postman" role (definitely in relation to data it does not process by itself), imposing unnecessary burdens on public authorities. Moreover, based on feedback, the transfer of data is not free of error, e.g. the NTCA and NHIFA records do not always match (e.g. in relation to the FEOR).
- **Data exchanges between public administration IT systems and records of public authorities are performed with heterogeneous technological methods:** The mass transfer of data is performed through an MQ channel, with DVDs, individual data are provided through individual data retrievals offered by the KKSZB (Central Governmental Service Bus); as a result, based on feedback, the quality of data replication between public authorities is inadequate (e.g. in the course of reporting, receiving, forwarding data on insurance, the up-to-date status of data is not always ensured

[9] EY-BI (2019), pp 22.

between the employer, the NTCA and NHIFA, resulting in substantial further data reconciliation duties for employers).

- **One-way reporting process:** Within the current system, employers do not receive relevant feedback from public authorities as to the specific data sent by them. This often leads to duplicate reporting aimed at averting the risk of omitted or incorrect reporting. The fact that employers are unable to retrieve data related to them in the official records also prevents employers from validating data themselves, which would in turn significantly enhance the reliability of data.

The key finding relating to the reporting process is that on the employer side, substantial administrative burdens are linked not to actual reporting, but to the preceding three steps.[10] This, however, does not reduce the necessity for comprehensively reforming the reporting system of employer data, as most of the above noted symptoms—a redundant system for other reasons as well—substantially impact the amount of preparatory activities, and as such, the actual degree of the administrative burden .

The table below assesses the above findings on the basis of two criteria. First, it assesses the extent to which the given factor is an important source of administrative burdens (based on expert estimates, on a scale of five), and second, it examines whether the given factor is manageable within the current logical environment. We distinguished three possible options for managing the suboptimal factor:

1) Manageable within the current logical framework by development of processes
2) Manageable within the current logical framework by IT development
3) Not manageable within the current logical framework

#	Suboptimal factor	Severity	Mitigation method
1	Form based reporting logic, not adapted to processes of enterprises	3	3
2	Very similar and partly overlapping information requirements	5	3
3	Use of different terms	4	3
4	Requirement of providing data available in public databases	4	2
5	Reporting with varying timing	2	3
6	High rate of incorrect reporting	4	3
7	Only limited functioning of online validation	3	2
8	Varying level of digitisation in the reporting process	3	2
9	Varying level of digitisation at employers	3	2
10	Outdated reporting systems	3	2
11	Wide range of secondary reporting	3	3
12	Data exchanges between public administration IT systems, records of public authorities are performed with heterogeneous technological methods	3	2

[10] After recognition of the above, the EY-BI study in 2019 also attempted to provide a breakdown of time spent on individual steps at the level of processes (assigning the relevant costs), but for the vast majority of respondents, the process was only meaningful to them as a whole.

#	Suboptimal factor	Severity	Mitigation method
13	One-way reporting process	13	One-way reporting process

Table 6: Assessment of suboptimal factors

The table gives rise to the following conclusions:

- Neither of the suboptimal elements we identified are manageable within the current logical framework purely by modification of processes or regulation.
- Substantial progress can also be achieved in relation to six of the thirteen factors through IT development within the current logical framework; this, however, is insufficient for the remaining seven factors, for which a logical paradigm shift is needed. An event-based approach can provide a genuine solution for these.
- In terms of severity, all of the most critical factors (a total of 5 factors with a value of 4 or 5), except for one, can only be managed with a logical paradigm shift .

In the light of these findings, a comprehensive reform is essential to have the right impact. A new data system could address the main problems identified along the following lines:

- Periodic data reporting is replaced by event-based data reporting, which adapts the data reporting process to the needs of the employer.
- Employers report only a narrow set of relevant event data to a single central system, linked to employee events (e.g. payroll, promotion), from which all relevant public bodies have access to the data relevant to them. In this way, the employer only has to report all data once, through one channel, eliminating the current redundancy.
- In the course of reporting a number of verifications need to be performed in relation to events (and potentially preventing reporting of incorrect data), which are currently performed by authorities after submission of forms. This way most verification functions would be reallocated to a time preceding data sending, which would significantly improve the quality of provided data and thereby prevent most subsequent corrections.
- Data contained in public administration IT systems should be channelled into the new reporting system. This would enhance verification efficiency, on the one hand, and reduce the reporting obligation of employers, on the other; employers would only have to report data not yet available on the State side.
- Among elementary event data reported by employers, all authorities should also be able to access data available to them in the past. This may result in substantial time savings for employers, as data are utilised in several cases, and is particularly useful in relation to statistical reporting to the HCSO, as employers would not have to understand certain statistical terms (e.g. in relation to staff size), for example.
- The IT solution supporting reporting should be adjusted to varying employer needs; a version integrated in payroll software and a web/mobile app is necessary for employers with lower levels of digitalisation. Digitalisation of the process, however, is essential in both cases.

- Reporting stakeholders should be able to access data related to them, stored on the State side, on the platform supporting reporting. This results in greater transparency and more efficient reporting.

3. Business requirements for the new data reporting system

3.1. Business expectations of the new system

3.1.1. Assumptions underlying business expectations

Assumptions are probabilistic facts that need to be validated during the design and are taken into account in architectural design decisions.

Assumption	Description of the assumption and its implications
Business assumptions	
Public authorities can continue to access data provided to them in the past.	We assume that within the new system, public authorities can continue to access data falling within their competence.
Employers are not required to collect data sets varying from the current ones.	In some cases, the new logic requires reporting entities to provide new data compared to previous data (that is, previous data in a new breakdown) to ensure that public authorities can compile the forms from data elements of events. Employers, however, are not required to collect completely new data sets.
A transitional period is expected, when the old and new reporting systems will operate in parallel.	Based on stakeholder expectations and benchmark related experience as well, a transitional period is necessary, when the two reporting systems operate in parallel. The transitional period can run in parallel with phased introduction in relation to both reporting and the scope of reporting entities required to provide new types of data.
Within the new system, (secondary) reporting between public authorities will not be necessary.	Since public authorities directly access relevant data within the new reporting system, the obligation of reporting between public authorities will cease.
All reporting currently in effect can be compiled from events.	Current reporting can be produced from event catalogue elements in an algorithmic manner; creation rules for necessary event sets can be defined.
Due to the single-channel function, a number of cases of reporting can be replaced.	Due to the single-channel function of event-based reporting, a number of cases of reporting can be replaced, as each relevant public authority can access relevant data at the same location.
The design of the event-based reporting system prevents certain errors from occurring.	Within the event-based reporting system, a number of data are generated as a result of calculations performed on the reporting platform, whereas these had to be calculated by data providers in the past. Owing to the above, the system prevents errors resulting from calculations; different content verification methods ensure that correct and authentic data are entered into the EMAP system during data reporting.

Assumption	Description of the assumption and its implications
The event-based reporting platform can replace communication between official public administration IT systems in the long term.	The event-based reporting platform offers the long-term option of replacing direct communication between official public administration IT systems, as it will contain various event data from which public authorities can directly produce data relevant to them. The "status flag" data in the specialised systems will be provided by the integration of the specialised systems with EMAP.
Technological assumptions	
Adapting the public administration IT systems to the new reporting logic is possible but time consuming.	Public administration IT systems operated by public administration bodies are currently prepared to process form-based declarations. To transition to the new data reporting model, the data loading logic must be modified. It is assumed that these changes can be made on the part of the public administration body, but this will take several months or even years.
Online data verification is a service that can be outsourced.	It is assumed that the verification logic built into the applications supporting data provision can be outsourced to reporting systems in the form of microservices.
The transformation of reporting systems can be enforced.	We assume that the transformation of systems supporting data provision (to handle the new event-based data provision) can be enforced by law, which affects both ▶ the logic (i.e., the use of mandatory and optional functions can be prescribed), ▶ and the accountability (i.e., the connection takes place in a regulated way, e.g. through system accreditation).
Employers' and public authorities' systems will be able to handle the mixed reporting model.	Employers' systems are assumed to be able to adapt to the transformation strategy (e.g., for a deadline or on a voluntary basis, but they will restructure the system). We expect the service supporting data provision to make it transparent for the public administration IT systems whether data is provided according to the new or old reporting logic.
The optimal operation of the system requires the development of official IT systems.	A rendszer bevezetésekor a hatósági szakrendszereket nem kell fejleszteni, az új adatszolgáltatási rendszer transzformálja a beérkező eseményeket a hatóságok által használt formanyomtatványoknak megfelelően, so that the necessary forms can be generated from the event data. The long-term goal is to replace the transformation form by allowing official public administration IT systems to process events directly. In terms of the administrative burden, this will be a real step forward.

Table 7: Assumptions about the new system

3.1.2. Main business goals and principles

Maximisation of benefits for data providers (and employees)	
Description	When reforming reporting relating to employment, in decision making we prioritise considerations of reporting entities and maximise business benefits in relation to them.
Justification	The primary objective of the development project is to substantially reduce burdens relating to reporting. Administrative burdens must significantly decrease to ensure acceptance of the new reporting system.
Consequence	Primarily software developers supporting reporting with IT solutions need to adapt to the new system; when determining the scope of work, it is necessary to consider that costs of further development increase the costs of reporting entities (software maintenance, licence fees, service fees).

Bodies requesting data may not request data already available to the State	
Description	Only data not available to any public authority may be requested from employers. If a public authority is already in possession of the given data, it is required to provide such data to the new reporting system.
Justification	This approach can ensure elimination of redundancy experienced by reporting entities in reporting.
Consequence	An appropriate technological and legal (data protection) solution must be found for the data sharing process between public authorities.

Compliance with data protection requirements	
Description	The new system should meet data protection requirements stipulated by legislation.
Justification	In the new reporting concept—irrespective of the technological solution—a central system will store all personal data relating to reporting, which raises a number of data protection concerns.
Consequence	Compliance with data protection requirements should be credibly demonstrated in the conceptualisation phase.

Implementation of appropriate legislative changes	
Description	The event-based reporting system requires wide ranging legislative changes.
Justification	Due to the new technological background, changed process, issue of authorisations and other aspects, the new reporting system is not functional without comprehensive legislative changes.
Consequence	Sufficient time should be provided for identification of legislative amendments and the codification process.

Multi-level verification	
Description	Multi-level verification functions operate within the event-based reporting system. Verification within the reporting system is aimed at filtering various types of errors.

Multi-level verification	
	Verification should follow reporting as soon as possible (ideally immediately, before acceptance), providing feedback to data providers.
Justification	Multi-level verification ensures that the event-based reporting system contains correct information at form and content level.
Consequence	When drawing up the system, complex verification algorithms should be integrated in the platform receiving events. Some of these should be accessible to data providers on the reporting platform or in offline mode.

Table 8: Business goals and principles

3.2. Operating model of the new system

3.2.1. Management of development and operation

Owing to its unique complexity, event-based reporting reform requires an active role from a number of public bodies. It follows that a central consortium management body should be established in both the development and operating phases. The Ministry of Finance (MoF) should continue to provide professional management of preparing the development project, but support at higher level is also justified to ensure success. Taking into account that the MoF does not possess necessary capacities for managing preparation of the development project, such resources should be designated or provided with external support in expertise. The project will be unsuccessful if adequate management capacities are lacking.

The authorities concerned should provide delegated resources and representatives in the form of a consortium in the project, which are actively involved in the development project, and support implementing parties and external experts. Proposed members of the consortium:

- Ministry of Finance
- NTCA
- HCSO
- HST
- NHIF
- Ministry of Interior
- Digital Hungary Agency Zrt. (or Cabinet Office of the Prime Minister)
- any other data hosting authorities

A government commissioner should manage the consortium, who can ensure efficient operation of various public bodies through operation of an interministerial committee. A government decree should also set out the consortium's rules of procedure.

The central management body is also essential in the operating phase. It should actively support EMAP developers by providing timely notification of possible legislative changes affecting the system and enabling them to commence necessary development. In the operating phase it is also necessary to divide duties managed by the consortium and assigned to individual authorities. Duties assigned to individual authorities (e.g. development projects related to their own specialist IT systems and forms) must be performed with their own appropriate resources.

3.2.2. Role of stakeholders

The role and scope of duties of stakeholders in the two phases of implementation and operation is described below .

1. **Duties arising during implementation:**

Employers

- Preparation for changes, identification of possible changes necessary in internal operation (in cooperation with companies providing payroll and HR systems, and external partners providing payroll and HR services).
- Testing of certain developed functionalities in relation to reporting through events to the EMAP.

Organisation responsible for implementing the EMAP

- Preparation and implementation of the EMAP implementation project.
- Establishment of consortium with key actors of implementation. Its proposed members: MoF, NTCA, HCSO, NHIF, HST, Ministry of Interior (MoI), the newly established Digital Hungary Agency Zrt. and all other relevant official data managers.
- Establishment of project organisation (dedicated resources and network of experts providing support).
- Acceptance, summary of needs and requirements defined for the system, channelling of such needs into development (where necessary).
- Coordination of creating a legal framework necessary for the solution to be developed (drafting and proposal of legislative recommendations, and coordination of communication related to establishing the legal framework).
- Updating of event catalogue and drafting of maintenance rules of procedure.
- Setup of the body operating the EMAP, which includes identification of individual stakeholders, determination of their functions, and the drafting and documentation of processes necessary for operation.
- Putting into service of infrastructure necessary for operating the EMAP and establishment of its operating conditions.
- Upon selection of a technological solution applying DLT,[11] preparation for operation of nodes with involvement of data processing bodies.

Bodies developing EMAP applications (suppliers)

- Development, delivery of components of the event-based reporting platform (EMAP):
    - Event-based web reporting system

[11] See Chapter 4.3 in relation to DLT (distributed ledger technology).

- Event handling system (creation of event catalogue, receipt and provision of event data)
- Data publication system
- Form transformation system
- Self-determination system
- Development of operational support services
- Integration duties (KAÜ (Central Client Authentication Agent), BKSZ (Secure Delivery Service))
- Drawing up of administrative duties

Public bodies processing provided data (NTCA, HST, HCSO, NHIF)

- Involvement in the implementation project according to rules of the project organisation.
- Collection, aggregation and forwarding of arising system requirements and expectations for the body implementing the EMAP.
- Implementation of development necessary for providing status indicator data.
- Feedback to bodies responsible for EMAP development during the entire period of development.
- Testing of developed system functionalities.
- Specialist IT system development (e.g. validation procedures, return of result status).

Organisations developing reporting systems

- Implementation of necessary development related to payroll systems, testing of cooperation with the EMAP, system accreditation.

2. <u>Duties arising during operation:</u>

Upon implementation of the event-based reporting system, due to the complexity of interconnection, integration and cooperation between the specialist IT systems, assessment of the management and regulation of professional and technological operation is a critical factor. Significant dependency evolves between interconnected electronic services and integrated specialist IT systems; their professional, technological, operational and development tasks cannot be covered efficiently with locally organised central management.

It is therefore necessary to complement the concept of organisational and professional management with administrative organisation, coordination duties necessary for the coordinated operation of IT systems operated by professional operators, involved in integration. A possible solution for managing this is the establishment of a body with central coordinating authority and professional competence, involved in reforming, overhauling the processes, drafting of IT development needs related to these, and in preparation of related legislative changes. Establishment of such central management body is essential for launching the project.

During operation, however, there are not only duties managed centrally by the consortium; the relevant bodies themselves need to provide, *inter alia*, human resources necessary for development related to individual authorities.

Body responsible for operating the EMAP

- Maintenance of the event catalogue, updating related to necessary modification needs.
- Technical management activities, e.g. operation of applications, databases, infrastructure.
- Maintenance of technical specifications for implementation of integration.
- Activities related to service life-cycle management.
- Duties related to change management: business requirements arising on the side of data subjects, management and implementation of development needs (e.g. implementation of legislative changes within the system, updating of verification algorithms, management of changes affecting the event catalogue etc.).
- Helpdesk activity for supporting users (L1).
- Technical support activities at lower levels (L2-L3).

Public bodies processing provided data (e.g. NTCA, HST, HCSO etc.)

- Reporting to the EMAP system (in the form of status indicators), thereby updating of status indicators.
- Collection of data from the EMAP system into state administration IT systems.
- Error correction, mainly involving filtering of incorrect data and management of their correction. Scope of responsibility for error correction should be defined in advance (e.g. data overwriting rights, identification of necessary consultation points).
- Definition and forwarding of change needs: upon indication of various development needs (e.g. upon legislative changes, need for changing verification algorithms), the authorities directly affected collect such needs and forward them to the body responsible for operation, and assist in testing developed changes.

Organisations developing reporting systems

- Implementation of necessary development related to payroll systems.

Additional reporting bodies (e.g. National eHealth Infrastructure, civil status certificate system)

- Event-based reporting of data in certain public databases to the EMAP with relevance for reporting by employers.

3.2.3. Identification in reporting

In current employers' reporting there is simultaneous use of several identification data, resulting in a significant administrative burden for data providers. There are two main reasons for using various identifiers:

- Clear identification of relevant private individuals, which precludes identification errors stemming from name identity and typos;
- Public bodies processing data use different identification data for identifying employees.

Event-based reporting needs to take into account these two criteria, but should aim at reducing burdens of data providers by minimising use of necessary identification data.

According to the proposed solution, in the course of reporting the employee is identified on the basis of the tax ID, social security number, and by the tax number for employers. Additionally, the Ministry of Interior and the Central Register (ÖNY) provided by Idomsoft Zrt. support the identification activity of public bodies. As a result, storage of additional identifiers related to employees is unnecessary within the EMAP, and reporting is also simplified for employers, as provision of two identifiers is sufficient. It is possible, however, that the employee does not yet possess a valid tax ID or social security number (e.g. third country employees). Since such cases comprise only a negligible share of reporting, reform of the process is not justified on such grounds. The problem is manageable with a separate sub-process during detailed elaboration.

Data provision of employers

Various groups need to be identified for presenting reporting by employers in practice. These are:

- Employers using payroll software;
- Employers not using payroll software;
- Accounting, payroll providers;
- Self-employed persons.

For employers using payroll software, reporting is performed through payroll software, enabling automatic employee identification through the tax ID (otherwise 4T identifiers) and the social security number.

For employers not using payroll software, they can provide data on the EMAP web platform. The figure below shows the identification aspect of reporting.

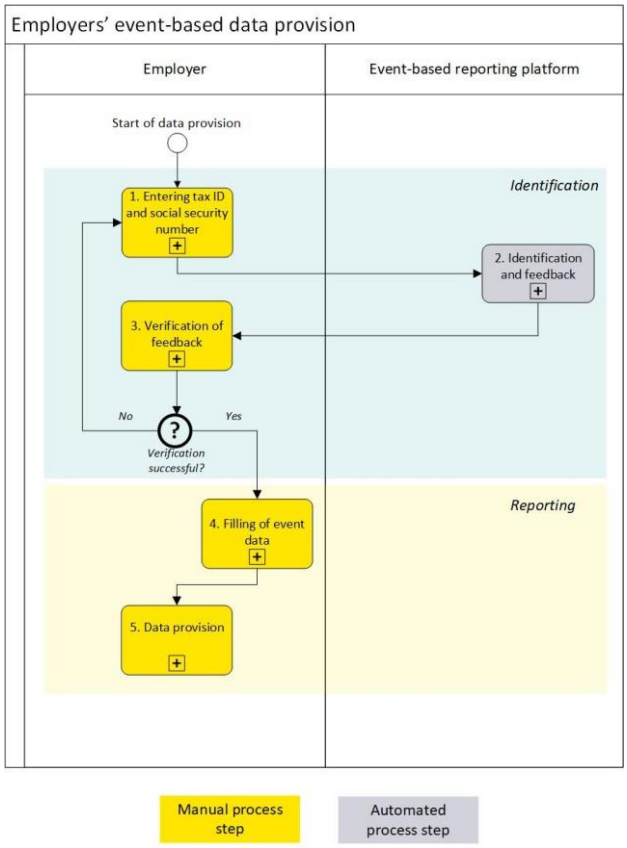

Figure 4.: Identification during employers' event-based data provision[12]

For identification of employees the employer first enters the tax ID and social security number (1). After pressing a button, the EMAP performs personal identification based on data, providing feedback on the result to the data provider (2). Identification, however, is successful only if the employee had already been registered with the employer, otherwise an error message is generated.

- If identification is successful (i.e. the employer provided correct data on a given person), the EMAP provides feedback on the employee's name to the employer. The employer can thereby confirm that it launches the event with appropriate identification data on the given employee (3).[13]
- If identification is not successful (i.e. the provided tax ID and social security number does not belong to the same person), the EMAP indicates this to the data provider with an error message (3). It is then required to again provide identification data (1).

After successful identification, the employer fills event data for the appropriate legal titles (4), then provides the event (5). The employer is not required to identify itself, as this is performed through EMAP user data.

The "Establishment of employment" (ETID-3-1) event is an exception in terms of identification, because for identification the data provider is required to manually upload all data, and the identification process verifies correct entry of all data.

[12] The figure shows the process for reporting agents without payroll software. If the reporting agent has payroll software, the steps are running automatically

[13] Although the system provides feedback to the data provider on the name of the person concerned, the data protection risk of the outlined system is reduced by the data provider's requirement to possess the private individual's tax ID and social security number. It is therefore likely that the data provider processes the private individual's data with his/her consent.

The reporting of accounting, payroll providers is similar, but identification of employees is preceded by identification of the employer. This is necessary because an accounting/payroll provider may provide services to multiple employers, hence it may not necessarily be possible to identify the given employer based on data on the EMAP user (reporting entities). The user registers the employer's tax number, on the basis of which the EMAP provides feedback on the employer's name, thus the user can verify the appropriate employer for data entry. It then identifies the employee by entry of the social security number and tax ID – the EMAP verifies whether the two identifiers belong to the same person. Related feedback is provided in the manner described above.

Identification is automatic for self-employed persons, as they are identified by the system as a user upon logging in to the EMAP platform. They are able to indicate on the platform the intention to provide data as a self-employed person; data provided by them will be automatically associated with them and beyond the login, they are not required to carry out further identification.

Identification performed by public authorities

Certain public authorities use various identification data for their own purposes; therefore the tax ID and social security number cannot be used in a uniform manner for identification of employees on the public side. Based on data protection considerations, however, it would be inappropriate to store all employee identifiers concerned on the EMAP.

The link between the Ministry of Interior and the Central Register (ÖNY) provided by Idomsoft Zrt. resolves this dilemma. The ÖNY aims to provide data exchange between specialist IT systems using different identifiers, thereby supporting services based on identification of natural persons.[14]

By way of the link between the EMAP and ÖNY, public authorities can continue to use their customary identifiers, while it is sufficient for data providers to use two identifiers. The process is illustrated by the figure below.

[14] https://idomsoft.hu/rolunk/termekeink/osszerendelesi-nyilvantartas/

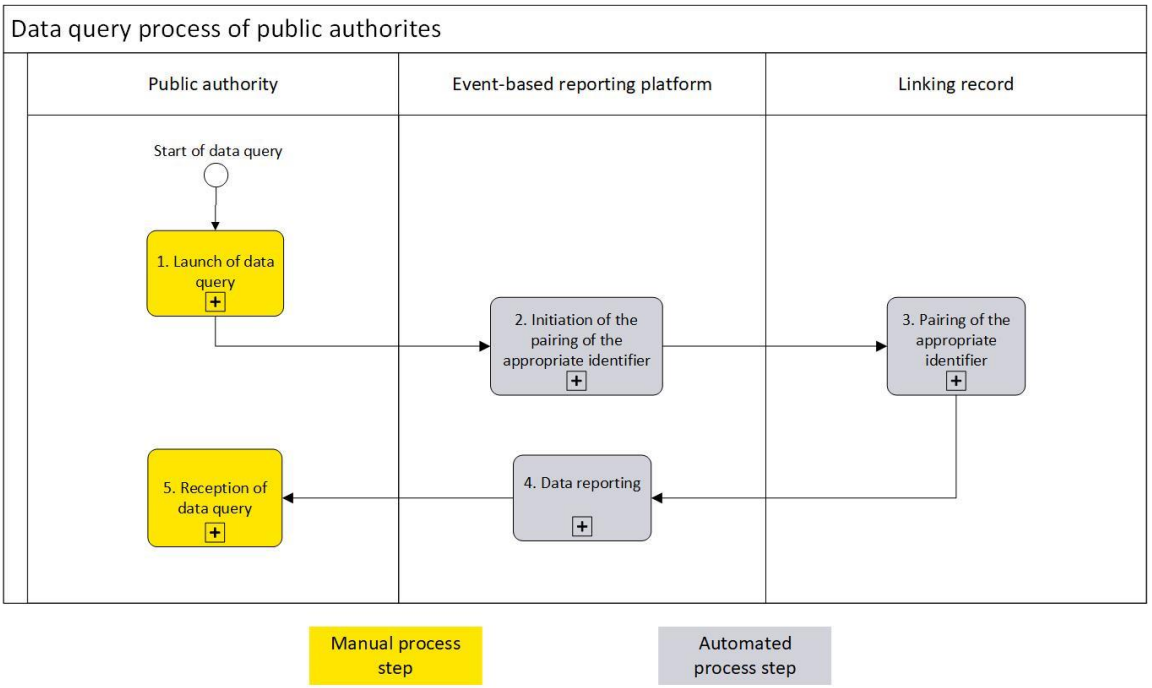

Figure 5: Identification during the data query process of public authorities

The public authority concerned launches data query on the EMAP (1). The EMAP indicates information as to which identification data are used by certain public authorities (2). Upon data retrieval, the EMAP retrieves identifiers used by the given public authority from the Central Register (3) and sends retrieved data with such identifiers to the users (4, 5).

Thus, in most cases, use of the Central Register will also be necessary for data retrieval on the EMAP by public authorities.

3.2.4. The reporting process

The following chapter presents the logic behind the reporting process within the new system and its main steps. To aid understanding, Chapter 8.1 includes a case study with a practical, straightforward example for illustration of the model and individual operational functions through some generally occurring events.

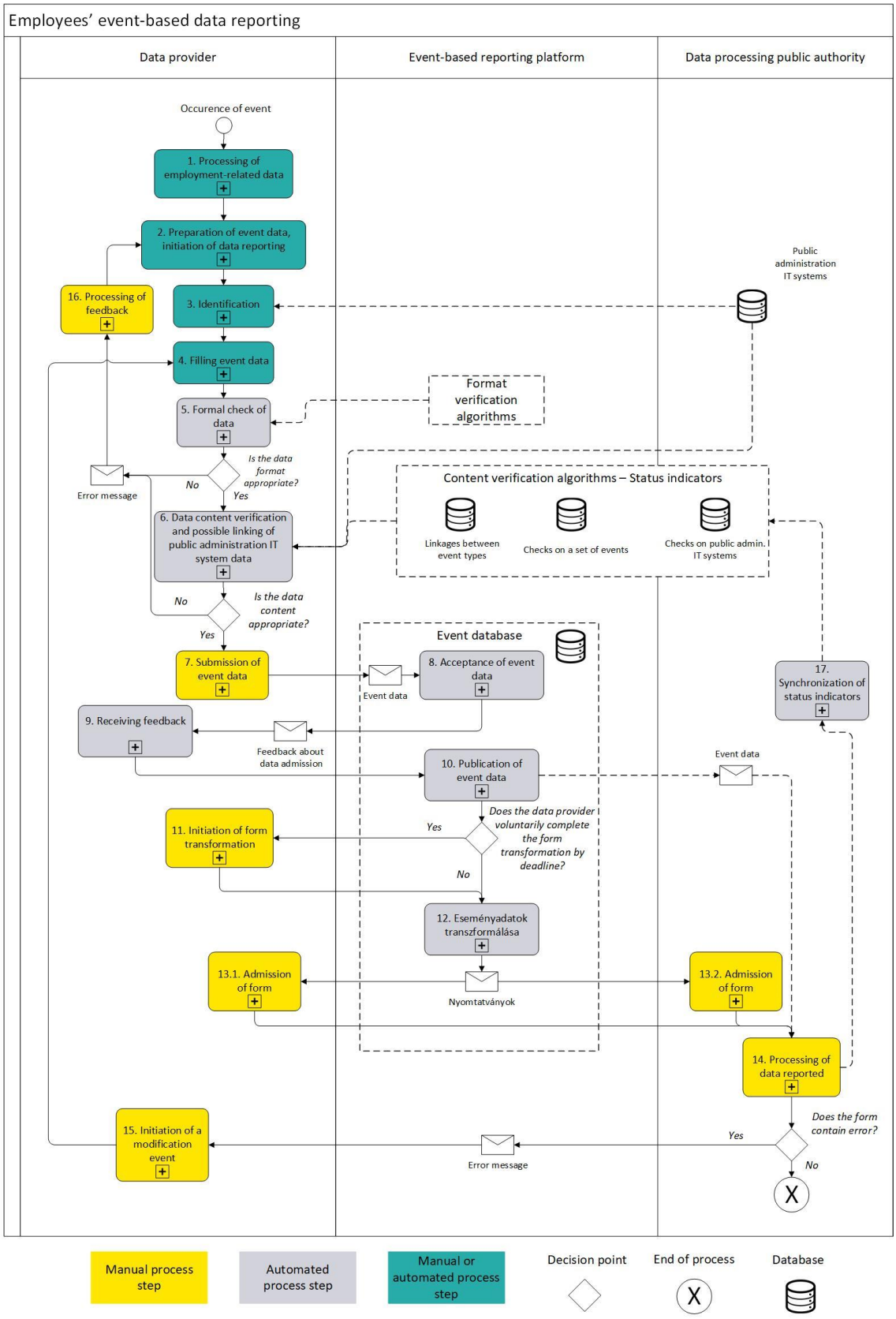

Figure 6: The process of data provision

0. Occurrence of event

- Occurrence of event related to reporting by the employer (see the event catalogue for itemised listing of events), which generates the reporting requirement.
- The event may occur
    - on the side of the employer (e.g. change in legal relationship, payments to employee), or
    - on the side of the employee (e.g. declaration on tax benefits, reimbursement of costs.

1. Processing of employment-related data

- Prior to event related reporting, individual actors are responsible for processing data related to various forms of employment. (Support of this step is not directly related to the event-based reporting project.)

2. Preparation of event data, initiation of data reporting

a) Initiation of reporting by the employer

- After the elementary event, the employer generates data of reportable events. Preparation may be carried out with software used by the employer (e.g. payroll system – if the functionality of the system used by the employer is suitable; in Excel), and on paper. Data to be sent can be generated three different ways, depending mainly on functionalities of systems used by the employer:
    i. Data are automatically generated in the employer's reporting software, if supported by the system. The employer can thus launch sending of prepared data from its own system to the EMAP through the events.
    ii. The employer exports a set of data, which it may upload through the EMAP web platform (or its application) during reporting.
    iii. Data necessary for reporting are manually, individually entered on the EMAP (web or mobile app) platform by selection of the appropriate event type.
- The employer initiates reporting. The process step may be manual or automatic, depending on the above noted conditions (i.e. whether it is performed by software maintaining an automated reporting connection with the EMAP, or by the employer).

b) Employee disposition over data on the EMAP

- Disposition over data stored on the EMAP can be divided into two different cases, based on data source:
    i. Data sent earlier to the EMAP by the employer (e.g. disposition over such data may be relevant when changing jobs)
    ii. Data transferred from the public specialist IT system (through specialist IT system connections) to the EMAP (e.g. marriage certificate data from the Electronic Civil Status System)
- The employee can check data stored on him/her and dispose over certain data (e.g. data related to certain rights) by selecting which stored data his/her employer may access among event data on the platform

3. Identification

- Before filling in event data, the data provider performs identification of the employee related to the event through the online services (periodic identifier verification is sufficient for one event type, e.g. once a month; the payroll software recognises validity of the identifier; see details in Chapter 3.2.2). Event data contents are uploaded after successful identification.

4. Filling event data

   - After successful identification, the data provider (or payroll software) enters event data content .

5. Formal check of data

   - Prior to the sending of event data, the system (as a service provided by the EMAP) performs formal check covering the following criteria:
     - whether all necessary (mandatory) data fields are filled in,
     - whether the method of completion is in conformity with formal requirements of event type(s) (whether content is in conformity with character limits of given fields – format and quantity limits)
   - To this end, the system matches the data fields to be filled in and their formal requirements with each event type. For verification it uses predefined verification algorithms provided by the EMAP.
   - If check detects a formal error, it sends an error message to the data provider and sending of the event is disabled. The error message contains the content (cause) and location of the error. In this case it is necessary to return to the beginning of the process, preparation of events and to correct the detected and indicated errors.
   - If formal check does not detect any errors, as the next step the system also performs substantive verification

6. Data content verification and possible linking of public administration IT system data

   During content verification the system first compares event data to be reported with authentic data ("status indicators") from public administration IT systems for the purpose of preventing the reporting of events that are invalid in terms of entitlement. It then compares the data of events to be reported with data of earlier events.

   - The number of incorrectly reported data can thereby be significantly reduced, as a number of verifications can be automatically performed prior to the sending of events, enabling the filtering of most potential errors in time.
   - Status indicators are the key attributes of employers and employees, which in most cases indicate an entitlement or contain master data. Status indicators show up-to-date, authentic data related to the current status, accessed by the system through links to individual administrative specialist IT systems. These ensure that the reporting system does not contain invalid events in terms of entitlement, identifying incorrectly provided data in such early phase of the process.
   - Three different forms of content verification may be identified (for the functionality of verification it is necessary to define verification rules for each event of the event catalogue in relation to all three types of verification; events in Chapter 8.1 contain an example):
     - **Verification of linkages between event types:** When the system reports events, it verifies links and correlations with earlier events (mainly verification related to entitlement). In relation to the event of wage payment, for example, it is necessary to verify whether the given employer reported the legal relationship earlier. To ensure completeness of such verification, it is necessary fully define correlations and links between elementary events. It is then necessary to map these dependencies within the EMAP system to ensure verification is run automatically.
     - **Verification of public administration IT system data:** With support from certain integrated public administration systems, the system compares data content of events to be reported with data (status indicators) of public administration IT systems through

provision of appropriate input data (mainly the tax ID, social security number, 4T data). Full definition of public administration IT system links is essential for ensuring complete verification (identification of available public administration IT systems and of data sets). It is necessary to define conditions of establishing public administration IT system links and to review such links during operation of the system to enable tracing of specific changes in legislation and in reporting. Verification of public administration IT systems may also extend to employee declarations submitted at former employers (e.g. enforcement at former employer in relation to the advance tax declaration of employees starting employment during the month).

- **Verification on a set of events:** Verification between elements of sets of events (performed locally, i.e. prior to the sending of data by the data provider) is necessary for jointly reported events. In relation to payments, for example, it necessary to prepare and "wait for" several types of events (deductions, contributions, benefits), then to run substantive verification between them; they can be subsequently jointly sent, once the system "gives the green light" to the data provider during verification. This type of verification ensures smooth transformation of forms later on. Possible errors are thus corrected before the sending of events, therefore the data provider does not need to correct other errors when generating forms.

- The status indicators contain the following data (their list requires constant reviewing and updating in the event catalogue, and depending on changes in legislation):
  - basic employer/employee data (necessary mainly to filter errors);
  - family status data (mainly data related to spouses for entitlement to tax benefits, data on children);
  - basic data of current legal relationship (date of reported/terminated employment, FEOR, working hours, data on changes to legal relationship);
  - status of incapacity for work (incapacity for work code, sick pay);[15]
  - data necessary for determination of benefits (FEOR, pension status, family benefit entitlement status, reduced capacity for work status, first marriage, personal benefit etc.);
  - company information (link with commercial register to filter errors).
- If the data content of the event to be reported is incompatible with the status indicators on the EMAP (e.g. the employer attempts to report wage payment to a person not reported as employed by it), the system rejects data provision with an error message, indicating the content (cause) and location of the error. Employers are thereby immediately notified of attempts to report data that are incompatible with data stored by authorities (e.g. if the employer failed to report the start of the legal relationship in relation to the given employee). In this case it is necessary to return to the earlier phase of the process and to again prepare the event to be reported, or, as the case may be, to prepare the reporting of a different event (e.g. if lack of a legal relationship generates the error, it is necessary to prepare the event for reporting the legal relationship).
- If verification does not detect any substantive errors, the elementary events are automatically accepted on the EMAP.

[15] If data are integrated in the EESZT.

- The data content of events may be supplemented with data of specialist IT systems simultaneously with substantive verification. This only affects certain events (e.g. when applying for the first marriage benefit, data on the spouse are matched from the Electronic Civil Status Register).
    - The reporting system thereby satisfies the need for not requiring employers to send data already available to public bodies.
    - This enhances enforcement of the principle of data minimisation, as employers (and payroll service providers) have to manage less personal data.
- When matching data from the specialist IT system, these are not redirected to the data provider; it only sees completion of the relevant data fields, but their content is not displayed.

7. Submission of event data
    - If verification did not detect any errors, the employer may initiate the sending of data.
8. Acceptance of event data
    - The EMAP accepts event data and provides feedback on this to the data provider on the EMAP, and to its notification storage in the transitional period.
    - The system generates a unique event identifier for the given event, indicating it in the feedback. Event identifiers are “revealing” codes, i.e. they refer to the type of event, thereby facilitating identification and subsequent searches.
9. Receiving feedback
    - The user of the data provider receives EMAP feedback on acceptance of provided data.
10. Publication of event data
    - After acceptance of events, event-based data become accessible on the EMAP, which, upon request, can be retrieved by authorised authorities, employers and employees without form transformation.
    - With use of a search field, the data subject provides the unique event identifier. If there is a hit, the given event may be selected, on the basis of which data of previous events can be viewed and data retrieval requests may be submitted, if the data subject possesses the necessary rights.

        a) Data retrieval initiated by the employer
            - After logging into the EMAP, the employer selects the appropriate data sets and group of employees whose data it wishes to retrieve from the system. Data retrieval based on event identifiers is also possible, when the employer can retrieve data on the given elementary event.
            - Thereafter the employer initiates data retrieval, which may be related to:
                - master data of employees, shared by them with the employer *(by provision of basic data/natural identifiers);*
                - events related to the given employee and their data *(provision of event identifier)*;
                - status indicator data (authentic data contained in individual specialist IT systems, retrieved by integrated specialist IT systems), e.g. data on legal relationships, data related to entitlement (payments, incapacity for work, entitlement to benefits) *(provision of data sets).*

- The employer receives feedback on the success of data retrieval and a list on the scope of possibly unsuccessfully retrieve data (if certain data sets cannot be accessed for the given person or an incorrect event identifier was provided).
- Data are exported from the platform in an authenticated form (data undergoing formal/substantive verification previously, or originating from an official specialist IT system, in the appropriate format for further processing (e.g. as an .xml or PDF file).

b) Data retrieval initiated by the private individual (employee)

- The private individual performs identification on the EMAP through the client gateway.
- After identification the employee selects the data sets to be retrieved (basic data; data on legal relationship; data related to entitlement etc.), which he/she may view on the EMAP or export from the platform in the appropriate format.
- Events related to private individuals and their data may also be retrieved.

11. Initiation of form transformation

- After acceptance of events, on the EMAP the employer may initiate transformation of events in conformity with current forms (if more reporting is not expected for the given period), on the basis of which it may receive feedback on whether the given form is completed by the submission deadline (earlier the system checked this through local verification), i.e. it presents the given form to the system.

12. Transformation of event data (form transformation)

- If the employer did not initiate transformation earlier, and authorities request data in the currently used form structure, the EMAP performs transformation of events in conformity with the forms after the prescribed deadline. (Chapter 8.1 contains an example for producing forms from earlier event data.)
- This is scheduled in advance, performed automatically, based on pre-established logic, linked to a triggering element (deadlines prescribed by law) – for forms in relation to which this is possible.

13. Admission of form

- The produced forms are automatically sent through the BKSZ, on behalf of the employer to the official portal of the relevant authority.
- The EMAP also sends the produced forms to the employer, indicating the events used for producing the form and the identifier related to the given form transformation (which is important for managing future modifications).
- This process step will be eliminated after the transitional period, once authorities can process event data by native means.

14. Processing of data reported

- Data processing by authorities will be performed in line with current practice, after retrieval of event or form data .

15. Initiation of a modification event; correction

- If modification, error correction is necessary, it may be performed on the EMAP through modifying events (modifications related to the legal relationship are an exception: establishment of a legal relationship is a key event, the modification of which is tied to separate events). The error may be identified by way of self-review or an error message received from the system; in the latter case

the employer processes the error message, then sends a corrective event in relation to the earlier event marked incorrect, with indication of the identifier of the event to be corrected. Formal and substantive verification is also performed in this case.

- After selection of the type of modifying event, the system offers the data content of events that may be modified. To this end, in the course of development it is necessary to fully determine which modification rules apply to the given event type in relation to all events, i.e. which attributes may be affected by the modifying events and which returns may be affected by modification (e.g. returns during the month). Such rules and list of attributes need to be determined for all elements of the event catalogue during the system design.
- Payments comprise a unique case, as the employer closes the period after payment, therefore such correction may be performed in the next period by payment/deduction of the appropriate amounts (Chapter 8.1 contains an example of a case and modification).
- The modifying event also affects various forms produced in the course of form transformation, as these may also have been produced with incorrect data. To manage these cases, a link is necessary between events and generated forms, on the basis of which it is possible to clearly identify the forms generated by the system in relation to the given event (e.g. the 08 return event) (or it is possible to indicate event data from which the given form was generated). For this it is necessary to also assign a unique identifier to the given transformation during form transformation, clearly enabling determination of which generated forms are affected by the error event (and modification thereof). Additionally, use of identifiers applied in the current process will also remain during the transitional period (form transformation): BAR code identifying correction and return identifier provided for correction.
- After receipt of the modifying event, the EMAP automatically sends notification to all authorities having used data of the original, incorrect event. The given authority can thereby retrieve correct event data and transformed forms.
- It is necessary to enable blocking within the system to manage closed periods in relation to certain sets of events, disabling subsequent modification of these. This is set individually for each employer, i.e. if the given company is inspected, the NAV indicates through official channels that blocking is in effect for the inspected period (and thereby for all events of the period). The system needs to allow lifting of blocking in certain predetermined cases, based on official decisions for certain actors and authorities (e.g. in relation to pension, the pension insurance authority needs to subsequently modify the event related to the 08 return).

3.2.5. Services

The new system improves the reporting system in relation to the following services.

- **Single channel reporting -** unlike the current reporting system, all relevant public bodies will report through the same channel, and public bodies will communicate back through the same channel.
- **Extended verification functions** – owing to the verification functions provided by the EMAP, more risks of error will be filtered in employers' reporting compared to the current situation (e.g. incorrectly stated legal relationships) even before the events will be reported. This will produce more reliable data for public authorities and reduce the number of subsequent corrections, which in turn will generate resource savings for both employers and public authorities
- **Decrease of burgen for employers** – since data elements are reported in the course of event-based reporting, public authorities may aggregate these as they see fit. Employers are therefore

not required to understand various conceptual definitions (relevant basic statistical terms of the HCSO) and different legislative changes (e.g. specific scope of fringe benefits), because the EMAP will be capable of calculating these from elementary event data. In addition, the new reporting system will allow for simplified identification, so that the reporting party will have to manage much less identification data.

- **Retrieval of data available to public authorities** – both employers and employees will have the opportunity to retrieve data on the EMAP relating to them. This will provide a clearer oversight of data possessed by public authorities. A query initiated by the employee can be used, for example, to check whether any tax benefits have actually been claimed when the monthly salary is determined.
- **Form transformation** – although event-based reporting provides data elements to the EMAP, a subsystem of the system transforms data elements to the currently used form structure upon the request of public authorities. With this function, data can still be forwarded to public authorities within the current form structure, even though reporting for employers is more simple, performed on an event basis. The function is considered temporary; it will be needed until the official public administration IT systems are switched to event-based data processing. The forms generated by the form transformation will also be available to employers, who can see which events have been used for which data fields in the forms.
- **Web-based reporting** – the event-based reporting system is by default connected to the payroll or accounting software of employers; therefore employers can report events through the software. Additionally, the reporting system also operates a platform accessible from a browser and mobile application, with which employers can use the system, if they lack payroll or accounting software.
- **Channelling of official data** – within the event-based reporting system, data generated by authorities, deemed to be public data, will play an active role in reporting. First, they will form the basis for EMAP integrated verifications, disabling submission of data in conflict with public data. Second, certain events also have data content found in official databases (e.g. data on children of employees). When reporting relevant events, the data provider will thus not need to also provide such data, as the EMAP will retrieve them from the relevant database on the basis of data related to the employee. This will significantly reduce burdens on employers, with the need for processing fewer personal data.

Reform of the reporting system mainly innovates processes for employers; its impact on public administration IT systems used by State actors is limited. In theory, however, it eliminates data exchanges between public bodies, as all actors can directly access relevant event/form data. During the detailed elaboration of the development project, however, it is necessary to assess sets of data for which access must be granted to EMAP content and whether there are current data exchanges that cannot be replaced with direct access.

The processing and generation of data on the State side, and the set of public administration IT system functions, databases and records will not change. Data generated on the State side are still deemed to be public data, forming the basis of verification, which can also be accessed by other State bodies through the EMAP, where necessary.

3.2.6. Applied events

As a basic requirement of the new system, applicable, however, only in the transitional period following launch of the system, it should be possible to prepare currently used returns on forms from the set of events, i.e. data loss should not occur. To this end, we have listed each data field of forms with relevance for the project, then determined events (or combination of events) matching the given data field. The resulting event catalogue – available in detail in Chapter 8.3 – contains all events (total of 20 events), including event types (total of 94 event types) to be reported by employers in the future. Types of events may include legal titles of varying number, each of which is matched with specific data content.

During reporting, event types are the base units to be sent. After selection of the relevant collection event, event and subsequently event type, and entry of identification data, the data provider can upload the data content of appropriate legal titles. The user can see legal titles related to the event type on a platform, and can thereby simply, simultaneously enter data for several legal titles, while it is sufficient to provide identification data only once. The user can add legal titles related to the given event type, for the event type to be sent with the "+" button. After pressing the button a new bracket appears with a drop-down menu, where the employer select the legal title in relation to which it wishes to provide data. The figure below illustrates this process and the possible layout visible to the data provider through the example of the ETID-1-1-1 event type (*"Remuneration for worked time"*).

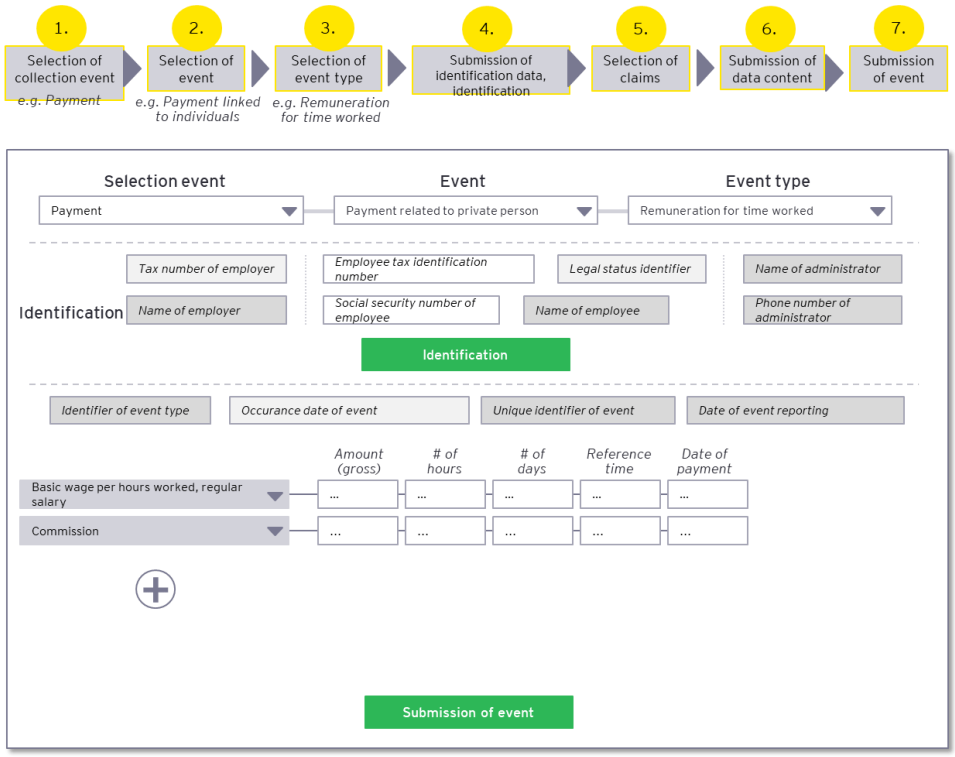

Figure 7: The layout of the data provision platform

Various data fields in the figure are marked with different colour:

- White fields are filled in by the data provider
  - Tax ID number of employee
  - Social security number of employee
  - Data content of event (Basic wage per hours worked, regular salary – Other work fee rows)

- Light grey cells are filled in automatically, where possible
    - Tax number of employer – if the employer provides data for itself, its own data are automatically uploaded. If, however, the payroll service provider performs reporting on its behalf, the tax number is provided manually.
    - Legal status identifier – if the employee has a legal status identifier with the given employer, it is uploaded by the system during identification. If the employee has several legal relationships, the data provider has to provide the given legal status' identifier.
    - Date of event – this field basically specifies the reference period. If the event type contains a data field for the reference period, the date of the Event is automatically filled in from this field. If there is no such data field, it must be provided by the data provider.
- The dark grey cells are automatically filled in
    - Name of employer – automatically filled in on the basis of the employer's tax number.
    - Name of employee – filled in on the basis of the employee's tax ID and social security number, if the two provided data belong to the same person.
    - Name and phone number of administrator
    - Event type identifier
    - Unique identifier of event
    - Date of event reporting

The figures below show the distribution of specific collection events based on event numbers, and types of events containing the most events.

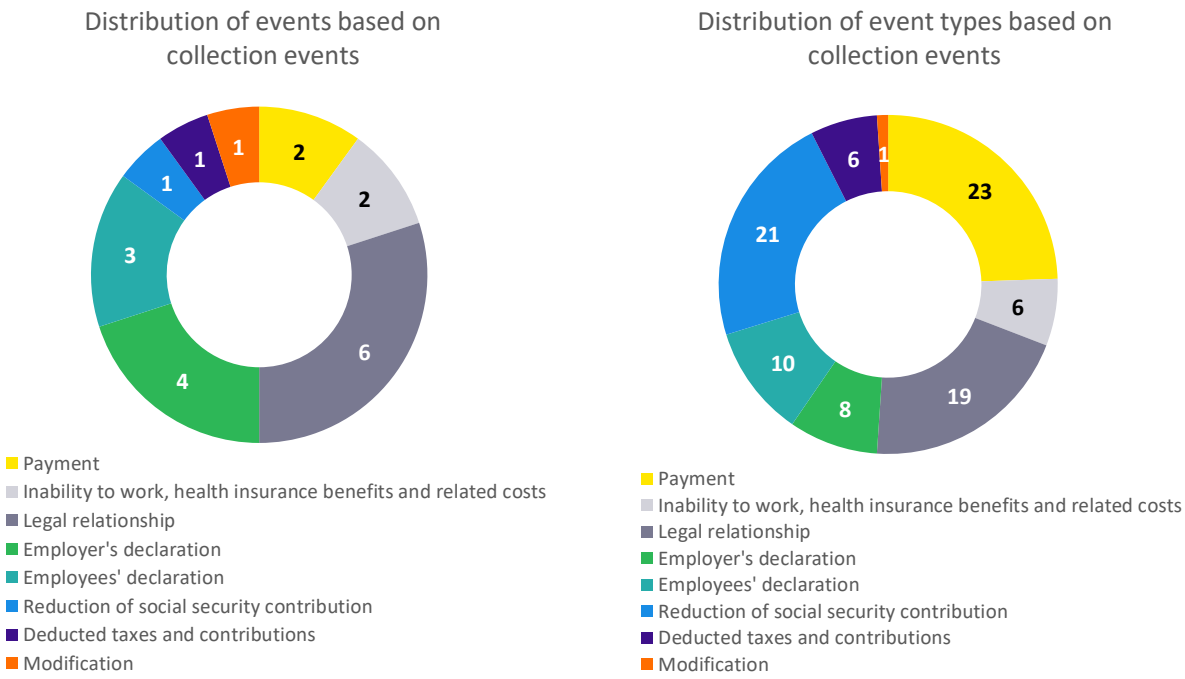

Figure 8: Distribution of events used by the reporting system

The table below details the number of elementary events (20), event types (94) and legal titles (273) within the event catalogue.

Collection event	Event	Number of event types	Number of legal titles
Payment	Payments related to private individuals	15	113
	Benefits not related to private individuals	8	8
Incapacity for work, health insurance benefits and related costs	Paid benefits related to incapacity for work	3	13
	Costs and deductions related to other cash health insurance and accident sick pay benefits	3	12
Legal relationship	Start of legal relationship	13	13
	Changes to legal relationship	1	1
	End of legal relationship	1	1
	Other legal relationship	1	1
	Cancellation of legal relationship	1	1
	Cancellation of cancelled working days	1	1
Employer's declaration	Rehabilitation contribution payment obligation	1	2
	Reporting by foreign enterprises	2	4
	Conclusion of collective agreement	3	6
	Declaration related to the coronavirus	2	4
Employee's declaration	Employee's declaration – Tax benefit	7	20
	Declaration on cost reimbursement	2	11
	Other declarations	1	26
Reduction of social security contribution	Effecting of social security contribution reduction	21	21
Deducted taxes and contributions	PIT – Contributions	6	15
Modification	Modification	1	1
Total		**93**	**271**

Table 9: Events, event types and legal titles aggregated in the event catalogue

3.3. Factors affecting project implementation

Development of the event-based reporting system is a very complex reform; the success and duration of its implementation is affected by a number of factors. We discuss below risks potentially underlying implementation and operation of the reform.

3.3.1. Factors affecting the implementation of the system

The ambitious schedule for introduction of the new reporting system – increasing related risks – is specifically called for by senior management. The time requirement of implementing the reform is influenced by a number of factors with only little room for manoeuvre.

- Coordination of technical, legal and professional criteria is time-consuming for achieving the serviceability of the complex system;
- Substantial time needed for authorisation and execution of the related public procurement procedures;
- Administrative requirements related to the programme may change depending on the type of financing.

In consideration of the above criteria, however, the time needed for implementation may be reduced with the following solutions:

- **Firm support of senior management** – in addition to adoption and approval of conceptual decisions, the senior management of relevant public bodies needs to provide appropriate support during project implementation. Owing to the nature of reform, a number of public bodies are affected, therefore large-scale cooperation is also needed on their part at different organisation levels. Senior management's firm commitment to implementation of reform may facilitate this process.
- **Efficient, flexible organisation and project management** – due to the broad scope of reform, during implementation it is necessary to coordinate progress of many sets of tasks, potentially spanning different fields. Disruptions caused by various links can only be managed with sufficiently flexible project management.
- **Segregation of development tasks** – the diverse tasks project a long development process. By segregation of sets of development tasks it is possible to launch development projects at different times, in coordination with each other, involving several developer teams. The scheduling of these tasks must take into account the requirements and timing of public procurement related to the project.

We identified the following risks associated with implementation of the reform.

Risk	Elaboration of risk *and its method of mitigation*	Risk severity
Delays caused by unreasonably complex requirements	The complexity of the technological solution's requirement specifications should be adapted to the planned schedule and costs of the reform. If the specifications are too complex, this may lead to higher costs on the developer side, which in turn may delay introduction of the reform. *The prepared detailed technological concept should be consulted with stakeholders, who are expected to play a role in developing the system.*	High
Higher costs during introduction and the transitional period	The transitional period involving parallel operation of the old and new reporting system is expected to increase costs. First, it is necessary to develop (payroll, human resource administration) supporting applications used by reporting entities, and second, it is also necessary for bodies receiving official reporting to develop the related IT applications and supporting infrastructure (primarily in relation to online validation in the short term). *The IT investments related to introduction of the system are necessary. For authorities, however, it is possible to phase the direct processing of event-based data, i.e. launch of the system is not conditional on direct data processing.*	High
The transitional period proves to insufficient.	Substantial time is required for transitioning to a conceptionally new system; if it is not available, the credibility of the entire initiative will be in doubt. *In consideration of the proposals of reporting entities, it is necessary to determine the length of the transitional period.*	Moderate
Difficulty of data protection regulation	Irrespective of the technological solution, compliance with data protection principles carries risk, as the new reporting system would store a large quantity of personal data. *In the course of the project it is necessary to identify critical points of data protection compliance, thereby laying foundations for a data protection impact assessment to be drawn up in the course of legal codification.*	Moderate

Table 10: Risks associated with implementation of reform

3.3.2. Factors affecting operation of the system

Risk	Elaboration of risk *and its method of management*	Risk severity
The new system does not access data available in related public databases.	Redundant reporting cannot be fully eliminated if the new system cannot channel data of related databases (e.g. the Personal Data and Address Registry in relation to personal and address data). This jeopardizes the feasibility of the in-built verification functions, too, as these partially rely upon official data. Without this, many error types cannot be ruled out automatically, increasing the burden both of authorities and employers. *It is necessary to identify regulatory and technical barriers to the linkage of public databases in such manner.*	Moderate
Public authorities can adapt to the new systems with varying degrees of flexibility.	In the planning and implementation phase it is necessary to take into account that the capacity to adapt and approach of different public authorities vary. *In the course of the project, benefits of the new system should be explicitly demonstrated to the relevant public authorities.*	Moderate
Limited business benefits in the beginning.	Upon introduction of the new reporting system, public authorities will not be able to directly process received events; these will be converted by a so-called form transformation module, adapted to the structure of current forms. This will significantly limit the expected business benefits for employers (e.g. fast feedback, fewer error messages that are easier to interpret). *To reach the full potential of the system, in the long term it is essential to develop the official public administration IT systems to ensure they can directly process events, therefore the disadvantages expected in the initial period are only temporary.*	Moderate
The integration of the reporting systems and the systems receiving the events impairs the efficiency of the employers' workflows.	The chosen integration solution affects how well the entire data provision process fits into the workflows of the employers. For example, in an asynchronous integration, it is difficult to determine when a response message arrives. *Technological possibilities and limitations must be taken into account when planning the reporting process.*	Moderate
Data providers experience the new reporting system as an increase in burden	The number of transactions (not number of data!) will multiply for both data providers and for recipients of provided data over current numbers. This will temporarily demand additional capacities on both sides due to modifications possibly necessitated by the learning process and rules of operation. *When designing the system, it is necessary to identify functions that may require additional capacities, especially on the part of employers. It is also necessary to continuously monitor simplification possibilities (e.g. inclusion of data of*	Moderate

Risk	Elaboration of risk *and its method of management*	Risk severity
	other specialist IT systems, expansion of the scope of verification). A pilot period operating with optional participants offers an opportunity for rethinking internal processes.	

Table 11: Factors affecting operation of the reform

The above detailed factors need to be managed for successful operation of the system, which will mainly be the responsibility of the body supervising the EMAP. To ensure adequate risk management, relevant public bodies need to provide firm commitment and support at the level of senior management. Additionally, when developing the EMAP technology, major emphasis must be placed on ensuring that the system is user-friendly and fast, which also enhances acceptance among data providers.

3.4. Long-term development opportunities

Although the concept outlined in the document represents operational reform of a unique scale in public administration, there is a number of additional development opportunities after implementation as well.

Integration of data on incapacity for work in the EESZT

Expansion of the EESZT with data on incapacity for work is a proposed development supporting efficient operation of the reporting system. Reporting and administration related to the incapacity for work would thereby be significantly more simple, easing the burden of both employees and employers. If, namely, data on incapacity for work would be registered by the GP in the EESZT:

- Paper administration related to sick pay and the document retention obligation of employers could be eliminated
- Real-time entitlement verification related to incapacity for work benefits could be implemented in the reporting process

To emphasize the importance of development, when presenting the concept below, we will also discuss the impact of implemented integration on operation of the reporting system.

Other development opportunities

The reporting system should definitely be expanded in the future with additional reported data currently existing on paper, including reporting to both public bodies affected by the reform and to new administrative/market actors. Such new data could be e.g. the M30 (annual tax certificate) and individual contribution certificate, reporting of income data comprising the tax base to banks and the KATA form.

Benefits of the EMAP can be further enhanced by channelling new public databases (e.g. vocational training data). This would expand verification preceding reporting, which improves reporting quality and reduces the number of subsequent error corrections.

The administration obligations of employers can be significantly reduced by integration of managing execution. The feedback of payroll specialists suggests that the current system of managing execution is extremely complex, requiring a lot of administration and lacking sufficient transparency for the relevant employees. Due to the complexity of processes, there is room for many errors, which imposes even greater burdens on stakeholders. One option for system integration is the role of the NAV in the process, where executors present their claims and their substantiation to the NAV, the latter forwarding the aggregate claim after their validation to employers.

4. The proposed IT architecture

4.1. Design principles and limitations

4.1.1. Design principles

Data principles

Retention of data in the very long term (in consideration of the retention period compliant with legislation)	
Description	Data on employment should be retained for the lifetime of the employee or for as long as the public services based on it are available.
Justification	The architectural design of the IT system should be future-proof, i.e. data access should be possible even one century later. Data cannot be lost under any circumstances. Technological, social, environmental, etc. changes should not disable access to or use of data.
Consequence	The chosen technological solutions should ensure data availability and offer technical solutions for data migration to other technological platforms also for very rare events.

Data sharing	
Description	Data are shared with relevant public authorities based on legal authorisation or the data manager's authorisation.
Justification	The single-channel reporting system is functional, if all relevant public authorities can access data within their competence within a central system.
Consequence	An appropriate authorisation management system should be drawn up to ensure that public authorities can only access data within their competence (in a decodable form).

Consistent data quality	
Description	The quality of data stored in the new reporting system is consistent.
Justification	The credibility of the reporting system is impaired if the quality of data is not consistent.
Consequence	Data within the system should be formally verified and substantively authenticated.

IT system principles

Product-independent architecture	
Description	The proposed architecture of the event-based data provision platform is independent of specific products of specific vendors.
Justification	Independence from the manufacturer or the product generates competition when selecting potential technical solutions during the implementation, which will make the design, operation and further development of the reporting system cheaper.
Consequence	The product-independent architecture may allow the selection of vendors and technical solutions that do not fit into the technological environment of the operating organisation. To reduce the risk of this ▶ technological standards need to be defined ▶ preference should be given to boxed or open-source products.

Independence from related systems	
Description	The event-based reporting platform is independent of the systems connected to it, the standard data provisions based on the event catalogue and the data dictionary are available via standard interfaces.
Justification	The event-based reporting platform must be disconnected from its associated systems to minimize dependency. Independence from the related reporting and processing systems gives a free hand to the operator of the future data provision system in terms of the content and implementation of the necessary changes.
Consequence	It has the consequence that, ▶ the data provision standards and interfaces to which data requesters must conform must be defined, incurring a development cost on the connecting side. ▶ to disconnect reporting systems and the public administration IT systems of data processors, services that ease the conditions for connection will need to be implemented.

Use of state records	
Description	Integration is needed with public registries that can provide the data that ensure the fulfilment of data provisions related to the employment of employees.
Justification	It reduces the reporting burden by not requiring employers to obtain and/or provide data that is already on the public records.
Consequence	The legal conditions must be created for the use of public records and developments must be made for data provisions. A dependency will be created on the services used.

Application of robust technology platforms	
Description	Robust hardware and software that can meet the expected performance requirements and availability conditions, and that have already proven their capabilities in practice in similarly critical use cases, should be used..
Justification	A mature technology environment, free of teething problems, can be the basis for a high-priority solution such as data reporting by employers. Due to the strict business requirements for the data platform, including security requirements, it is not possible to experiment. However, this principle does not preclude the use of innovative technologies to solve subtasks such as ▶ they still contain many hidden security bugs that pose a security risk ▶ there are hidden pitfalls that hinder later development and changes ▶ competing implementations are available and there is a risk that a version is selected that will be discontinued later
Consequence	It is a limitation in the wide-scale use of cutting-edge technologies, especially regarding the implementation of the functions of critical nature.

Maintainability	
Description	The architecture of the system should allow the necessary maintenance activities to be carried out over the long term. The feasibility of this should be ensured independently of any organisation or person, with appropriate expertise, while respecting the expected service levels. .
Justification	Without the maintenance required to maintain IT operations, the system cannot be operated at the expected level of service.
Consequence	Technological solutions that are not prepared for live operation cannot be used.

Available skilled human resources	
Description	In terms of the technological solution, a suitably qualified and experienced expert capacity at a reasonable cost should be available. Expert training opportunities should be available so that the lack of qualified human resources does not hinder the development and operation of the technology.
Justification	Due to the long life cycle of EMAP, it is expected that there will be a continuous need for further development of the system. The availability of appropriately qualified human resources (experts) is necessary to ensure a high quality of development and operation.
Consequence	New or less widespread technological solutions without an extensive expert background cannot be used. Taking into account the life cycle of the technologies used, it is necessary to ensure the supply of new specialists.

Applying a technology that can track changes	
Description	The technological solutions chosen must allow the system operator to keep up with technological changes by modifying or replacing the system.
Justification	During the long life of the system many changes can take place that the operator has to manage by administrative (e.g., manufacturer support) or technical measures (e.g., replacement of cryptographic algorithms, replacement of the entire system).

Applying a technology that can track changes	
	Organizational and technological dependencies that leave the system operator vulnerable and place a significant financial burden on the operator cannot be allowed to develop.
Consequence	For all administrative and technical decisions, the long-term consequences must be considered, and the lifecycle of the system component and the exit points must be planned in advance.

Loosely connected interfaces	
Description	Systems cooperating in the employers' data provision should be loosely connected.
Justification	Interfaces between systems must be designed in such a way that the malfunction of one system or system component does not interfere with the operation of the other components of the system.
Consequence	Loose system connectivity limits the ability to serve use cases based on real-time collaboration.

Infrastructure principles

Use of central electronic services	
Description	Consideration of the use of available or planned future SZEÜSZ, KEÜSZ services.
Justification	The use of SZEÜSZ and KEÜSZ services developed and operated by the state is a cost-effective way to implement the required functionality, so no system components with the same functionality would be created.
Consequence	The system will depend on the SZEÜSZ, KEÜSZ services, so it must be adapted to them. It is not allowed to establish a direct link between EMAP and other public sector schemes. Public sectoral systems linked to EMAP should also develop services published on the SZEÜSZ/KEÜSZ.

Use of Government Data Centre (KAK) Services	
Description	In the case of public authorities, efforts should be made to ensure that the technological components created will operate in the KAK.
Justification	It is a central government effort and a legal requirement to use the KAK as the infrastructure centre for IT services. The KAK meets the security level required by the security classification of the system and the requirements for the expected level of service. The KAK fulfills the security level expected by the security classification of the system and the requirements for the expected quality of the service.
Consequence	The use of machine rooms and IT infrastructure operated by the public authorities will be limited. It is necessary to adapt to the technological and service regulations and restrictions prescribed by KAK.

4.1.2. Design limits

Design limits are exogenous factors limiting public bodies, the EMAP implementing body in achieving the set goals of employer reporting reform by application of a specific approach.

Transition of public administration IT systems to event-based reporting is independent of EMAP implementation	
Description	Transition of administrative specialist IT systems to event-based reporting may not affect implementation of the EMAP. The systems are receiving reported data in the current data structure, until these are modified.
Management	The EMAP needs to be adapted to expectations of administrative systems in relation to both data structure and the technical parameters of messages.

Public procurement procedures	
Description	EMAP implementation requires procurement of various equipment and services in accordance with public procurement procedures in force. Public procurement is a time-consuming process that is rigid in terms of change management.
Management	Compliance with public procurement rules is a major design criterion to be considered when planning the content, dependencies and schedule of public procurement packages.

4.2. The technological concept of the future system

4.2.1. Basic operation of the system

The central element of the proposed IT architecture is an Event Management Platform (EMAP), which

- provides a common communication channel between employers and public organisations for sending and receiving data required to complete event-based data reporting related to employment,
- gives employees the opportunity to share their data with their employer, or
- will be a trusted repository of employment-related event data, from which both employers and employees can check data on previous employment data submissions. The data will be retained for the period and shared in the manner required by law.

Actors of EMAP:

- An employer that receives and sends event data to complete the data reporting using the data reporting system in its own use, either via a direct machine-to-machine connection or via the user interface provided by EMAP.
- The public data-processing organisation(s) that receive and process the employers' data through their specialised administrative systems (e.g. NTCA).
- Reporting public organisations that provide valid data to support the provision of employment data.
- An employed person who provides employment-related data to his or her employer has access to and processes data relating to his or her own personal events.
- An organisation operating EMAP, which performs development, operational and customer service tasks, thus ensuring the conditions for the system's operation. It does not perform any data management activities.

The amount of personal data processed by EMAP (almost the entire population of Hungary is concerned), the nature of the data (e.g. personal and sensitive personal data), the long life cycle of the system, the impact of the confidentiality, integrity or availability of the data in case of a breach, justify the amendment of the Ibtv. Level 5 security classification under Ict. The EMAP security functions and the EMAP operating organisation shall jointly meet the security requirements.

The conceptual architecture of EMAP is illustrated in the figure below, which identifies:

- The actors who are the entities carrying out the data management and processing;
- The building blocks of the architecture that implement the capabilities of EMAP, in the form of system components that implement a set of functions;
- The relationships between the components of the architecture.

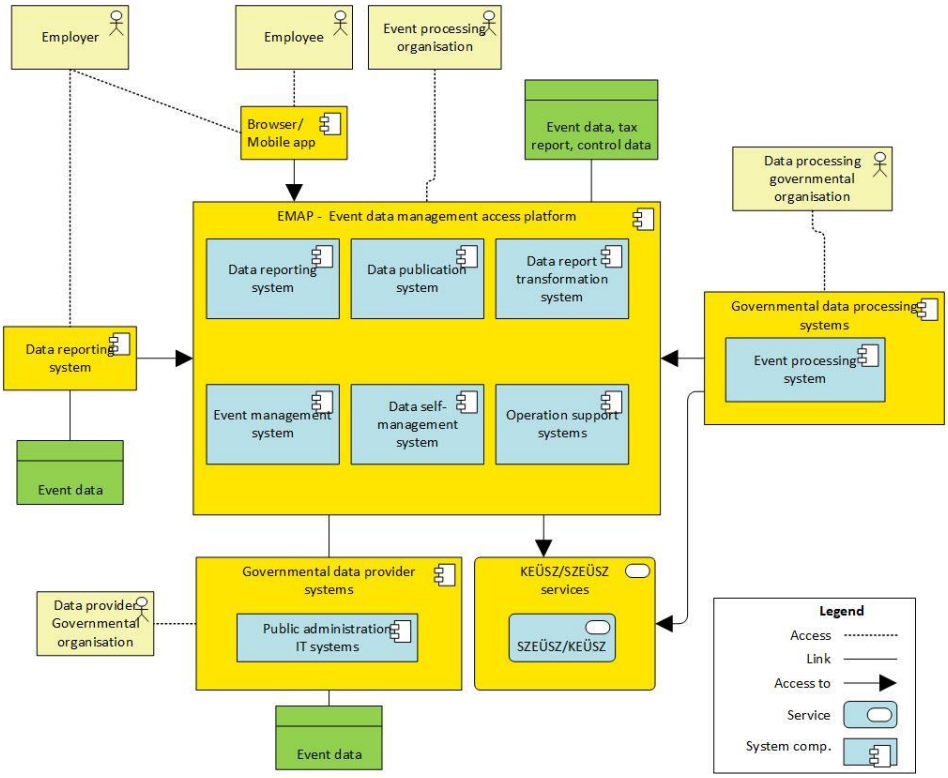

Figure 9: Concept of the event-based data platform architecture

The following table shows the building blocks of the EMAP conceptual architecture.

Architectural building block	Description
Reporting system	The reporting system is an IT system operated by the employer, independent of the EMAP; its main task is to generate data necessary for statutory reporting and to submit these to the EMAP in conformity with the required technical parameters. The reporting system also supports other duties of the employer (e.g. human resources management, payroll etc.) relating to employment and reporting by employers. The reporting system uses the services published by the EMAP, offered for reporting by employers through a machine interface or on the EMAP web platform with a user.
EMAP - Event-Based Reporting Platform	The event-based reporting platform is a modular system implementing single-channel reporting that ▶ Supports the employee in ensuring reporting by the employer, for which it makes available data, and formal and substantive verification rules. ▶ Supports the employee in reporting to the employer, and, where necessary, is involved in obtaining authentic data necessary for this purpose from the public administration IT systems. ▶ It supports public bodies processing reporting by employers by o Verifying the quality of reporting and uses data from the public administration IT systems for this purpose

Architectural building block	Description
	o Making available relevant event data to data processing bodies by native means or by transforming returns currently used on paper. The EMAP will be an authentic register of data reported by employers for all parties involved in reporting and processing, enabling the tracking of the entire life-cycle of reporting. The EMAP functionality is implemented by several application components described below.
EMAP reporting system	The EMAP reporting system provides services to employers and employees for reporting by employers. Services provided by the EMAP data provider: ▶ Full support of event-based reporting by the employer through a machine interface or web platform. ▶ Support of reporting by employees to employers (e.g. declarations) through a web platform or in a mobile app.
EMAP event handling system	The EMAP event handling system accepts, authentically stores and serves event data. Services of the system component: ▶ Management of master data o Event catalogue management: registration of business rules necessary for elementary event types and event-based reporting. o Management of return form catalogues: registration of the forms of returns generated by the EMAP and of business rules necessary for form-based returns o Management of master data necessary for operating the system ▶ Storage of event data o Acceptance and authentic storage of event data o Serving of event data, serving of the data requirement of EMAP components o Acceptance and authentic storage of data related to the processing of reported data (e.g. status data, receipts etc.).
EMAP data publishing system	The EMAP data publication system ensures the availability of the employment related data provision data to the entitled actors Services of the system component: : ▶ Publication of the data of the events submitted by the employers and the declarations generated as a result of the form transformation to the data processing organisations, ▶ Publication of messages sent by public data processing organizations (e.g., error list) to employers, ▶ Publication of system messages (e.g., receipts) for the parties involved in the communication Publication to the employer of the data provided by the employee Publication of historical data relating to the provision of data by the employer

Architectural building block	Description
EMAP Browser/Mobile app	A web and mobile application for employers and employees to use the EMAP data provider and the EMAP data publication system.
EMAP form transformation system	The EMAP form transformation system is a transitional component,, which produces the data required by the specialised administrative systems of public data-processing organisations from the event data in the form of the currently widespread form-based declarations.
EMAP self-provision system	The EMAP self-provision system component records the authorizations granted by employees, regulating the sharing of employee-related data with employers.
Systems supporting EMAP operation	System components that support EMAP provide technical and security-type services: ▶ Integration services ▶ Workflow control ▶ Identification and access management ▶ Logging and log management
State data provision systems	It is the responsibility of the public administration IT systems to submit data on specific events to EMAP based on the employee's authorization or automatically if required by law.
Public data processing systems	Specialised public administration systems operated by public organisations that process data ▶ receive and process the employment related data provision in native event format or in the form of form-based returns ▶ provide status information for the checks required to ensure compliance with the employment related data provision.
KEÜSZ/SZEÜSZ (Central Electronic Administration Services / Regulated Electronic Administration Services)	From the KEÜSZ/SZEÜSZ services, the following features will be used directly: ▶ KAÜ, to identify and authenticate system users ▶ KKSZB to achieve integration between EMAP and other specialised public administration systems

Reporting system

As regards the basic requirement of the EMAP, it should be able to perform event-based reporting by employers under conditions prescribed by law and with technical parameters specified by the EMAP operator.

It is necessary to prove conformity with the quality criteria of reporting.

The developer of the reporting system must take into account the quality criteria published by the EMAP operator.

The employer or developer of the reporting system may freely decide to use other services offered by the EMAP, which are not directly related to reporting.

The reporting system – depending on implementation –

- May be integrated with the EMAP, when it uses services published by the EMAP on a machine interface, or

- Is not integrated with the EMAP, when it only generates data necessary for reporting and reporting is performed with human user involvement through the EMAP web or mobile app platform.

Mandatory functions of the reporting system necessary for reporting by the employer[16]:

- Event catalogue management: The reporting system must at all times adopt changes in the event catalogue
- Generation of event data matching the event type, with the content and format prescribed by law, in conformity with technical parameters prescribed by the EMAP operator
- When generating event data, it should use the verification algorithms prescribed by the EMAP operator
- Managing the set of elementary events that correspond to a business event
- The system with EMAP integration in relation to reporting
    - It uses the formal and substantive verification algorithms made available by the EMAP (for sets of elementary events and elementary events corresponding to business events)
    - It manages error alerts generated during formal and substantive verification
    - It performs reporting by sending elementary event data in conformity with formal and substantive requirements, and business rules to the EMAP
        - It receives data sent to the EMAP, related to their processing, e.g.
        - Status data: Delivery, read receipts etc.
        - Error reporting related to the returns in the transitional period
        - Data processing bodies receive error lists generated during acceptance of events and official checks
- The system integrated with the EMAP downloads data necessary for reporting by the employer, addressed to the employer on a scheduled basis or upon the initiative of the user, e.g.
    - Data of declarations of the employee or data certifying these, stored on the EMAP or verified with use of the EMAP
    - Data of events shared by the employee and stored on the EMAP, status indicator data.

EMAP reporting system

The EMAP reporting system provides two types of interface for reporting:

- a machine interface (API) for the employer's reporting system, enabling provision of data to authorities with the EMAP services published there,
- web interface (web application or mobile app)
    - for employers to perform manual reporting, or
    - for employees to report to the employer.

The web application and the mobile app

[16] The EMAP is not responsible for ensuring that the reporting system generates all data necessary for reporting prescribed by law.

- are equivalent to the reporting system used and operated by employers, which are developed and maintained by the EMAP operator on behalf of the public and made accessible to employers not possessing a reporting system integrated with the EMAP.
- in relation to employees, the EMAP reporting tool is a web application through which they can perform data processing tasks necessary to ensure reporting by employers.

System component services for employers:

- Reporting of the employee to the employer:
    - Data of declarations made by the employee (e.g. declaration on division of tax benefits)
    - Data substantiating declarations of the employer obtained from other official administrative specialist IT systems by use of the EMAP (e.g. certification of entitlement to tax benefits)
    - Data of events shared by the employee and stored on the EMAP
- Reporting by the employer
    - Registration of event data on the web interface: registration of business event data or a set of events equivalent to a business event by uploading of files or the registration of data.
    - Formal and substantive verification of event data:
        - Verification of recorded data using algorithms provided by the EMAP.
        - Display of errors detected during verification
    - Sending of event data
    - Data related to reporting and processing:
        - Status data: delivery, read receipts etc.
        - Error reporting related to the returns in the transitional period
        - Data processing bodies receive error lists generated during acceptance of events and official checks

System component services for the employee:

- Registration of declarations for the employer,
- Retrieval of event data from the administrative specialist IT systems of other authorities, necessary for substantiating declarations.
- Sharing of event data stored on the EMAP with the employee, e.g.
    - Data sharing upon establishment of legal relationship;
    - Data certifying entitlement to benefits.

EMAP event handling system

The EMAP event handling system component receives, stores in an authentic form and serves event data for other EMAP system components.

The event handling system will be the authentic storage location of event-based reporting by employers. Technical solutions need to ensure that the conformity of parameters of reporting and the integrity of sent data can be authentically evidenced for all parties concerned at any future time.

Services of the system component:

- Managing an event type catalogue: managing elementary event types and sets of elementary event types associated with a business event, related business rules, versions, permissions etc.
- Registration of the catalogue of return forms: Registration of the properties of forms generated by the EMAP, e.g. their data content, relationship between events and returns, verification rules (event transformation rules, rules for verifying data content of returns), form transformation rules etc.
- Provision of verification services to accommodate machine and web-based online reporting: formal and substantive verification of event data using business rules and status indicator data,
- Acceptance and authentic storage of event data and data related to the reporting life-cycle (e.g. status data, receipts etc.) in respect of the following system components:
    - EMAP reporting system
    - Public administrative data processing IT systems
    - Public administrative reporting systems
- Supply of event data to satisfy the data requirements of the following system components:
    - EMAP Reporting System
    - EMAP data publishing system
    - EMAP form transformation system

EMAP data publishing system

The EMAP data publishing system satisfies the information requirements of EMAP users (employers, employees, public data processing bodies).

It performs two types of reporting tasks:

- Managing the forwarding of data related to reporting by employers (output channel management),
- Satisfaction of historical data retrieval requirements related to reporting by employers

The data publishing system uses data from the event repository managed by the EMAP event handling system; it processes and publishes event data by application of business rules defined for events and return forms.

Services of the system component:

- Publication of data on events submitted by employers to data processing bodies, which download data on events addressed to them,
- Publication of messages sent by public data processing bodies (e.g. receipt certificate, incorrect reporting) to employers who download data of messages addressed to them,
- Publication of system messages (e.g. receipts) related to messages generated in connection with the sending and receiving of events for the communicating parties, who download messages addressed to them

- Publication of event data for the form transformation component, for producing returns
- Publication of returns for data processing bodies (actual performance of return-based reporting on behalf of employer).
- EMAP users retrieve data of events related to them.

EMAP browser/mobile app

The EMAP browser/mobile app enables web access to services of the EMAP data provider and EMAP data publishing system components.

The two system components are the browsing software run on user devices or the mobile app installed on mobile devices, and are not part of the EMAP central systems.

Thin Client application run in the mandatory system component browser, through which reporting and management of data stored on the EMAP is possible.

The mobile app is an accessory with optional services optimised for mobile devices.

EMAP form transformation system

The EMAP form transformation system component is necessary until the administrative specialist IT systems of public data processing bodies are prepared for accepting and processing native event data.

Reliable operation of form transformation is critical in terms of its involvement as intermediary actor in fulfilment of employers' reporting obligations. The sending of event data and form transformation are performed separately in time, therefore, as a prerequisite of reliable operation, when accepting event data it is always necessary to verify whether there are obstacles to form transformation in the future.

For generating data of returns, the system component applies verification rules stored in the form repository, defined for individual forms.

It generates a data set from event data upon request by the employer or on a scheduled basis, which is in conformity with the data structure and data content of declarations based on current forms.

EMAP self-determination system

The EMAP self-determination system manages provisions of employees on data related to them:

- Maintenance of employee master data (typically personal data), their sharing with the employer
- Management of notification rules – selected events and means of communication used for notification of the employee

Systems supporting EMAP operation

System components supporting EMAP operation provide the platform necessary for operating business services and security services. These specified system components are separate from system components supporting operation, which support operation of the EMAP infrastructure.

The capabilities expected of the system components are not specific to the EMAP, therefore they should be composed of standard "boxed" and ready system components available on the market, which can provide the necessary services.

Platform services necessary for operation of the EMAP:

- Integration services supporting integration between internal EMAP components, and the EMAP and external systems connected through a machine interface:
    - Management of official specialist IT systems necessary for obtaining data required for reporting by employers
    - Publication of services necessary for reporting by employers (e.g. verification rules, retrieval of status indicator data from public official systems or the EMAP event handling system)
    - Support of the integration of specialist IT systems of public data processing bodies for accessing event and return data published by the EMAP.
- Workflow control that manages the execution process of tasks initiated or scheduled by the system's active entities:
    - Forwarding of reporting by employers
        - To data processing bodies
        - To the data publishing system
    - Form transformation control
    - Request of data from reporting bodies for reporting by employers

Security services necessary for secure EMAP data processing:

- Identification and access management services aimed at identification, authentication of active entities and regulation of their access rights.
    - Management of identity life-cycles: identity of each active entity must be registered and verified during use of the system. Active entities (e.g. users authorised by employers, employees, who are natural persons, devices, machine users etc.)
    - The authenticity of active entities should be verified with own internal authentication procedures or with Central Client Authentication Agent authentication in relation to natural persons
    - Support of role-based access model capable of managing access to data in consideration of authorisation provided in legislation or within the system
- Use of cryptographic services (e.g. encryption, electronic signature, time stamp, blockchain etc.)
    - Protection of the confidentiality and integrity (including authenticity) of data, when these are stored or moved.
    - Ensuring the authenticity of reporting, transactions
- Services supporting logging and log management, which support monitoring of user and system activities on the EMAP:
    - Generation of log data tracking the entire reporting process
    - Generation of log data documenting access to data

Public reporting systems

The public reporting systems provide authentic data through the EMAP for reporting by employers.

- Employees initiate the retrieval of data from the relevant public reporting specialist IT system (e.g. certification of the number of children from the EAK (Electronic Civil Status Certificate)), which are shared with employers for substantiating reporting.
- During reporting by employers, the EMAP retrieves data from public administration IT systems for verification of event data.

The chapter Interfaces contains the scope of data originating from external sources used in reporting by employers and the relevant public reporting systems.

The EMAP uses services published by the public reporting systems, if these are available, otherwise it is necessary to upgrade the public administration IT systems.

Public data processing systems

The public data processing systems related to the EMAP currently receive data of form-based returns, which are directly sent by employers through the Company Gateway or Client Gateway.

For event-based reporting by employers, the employer provides data by sending to the EMAP, and the EMAP is responsible for forwarding data to public data processing systems:

- In the form of native event data, if the public administration IT system is prepared, or
- In the form of data sets with content corresponding to form-based returns generated by the form transformation system component.

In relation to reporting, the public data processing systems

- Send event data to the EMAP on receipt and acceptance of reporting by employers (note: this is the default procedure for specialist IT systems processing native event data, and an alternative of the Central Governmental Service Bus (KKSZB) for the public administration IT system processing form-based reporting.

KEÜSZ/SZEÜSZ

The Central Electronic Administration Services / Regulated Electronic Administration Services (KEÜSZ/SZEÜSZ) services available to the EMAP will use the following:

- The KAÜ for identification and authentication of natural persons using the system, when they connect to the EMAP or before required operations;
- The BKSZ for delivering form-based returns;
- The KKSZB to achieve integration between EMAP and other public administration IT systems.

4.2.2. Interfaces

This section describes the interfaces between EMAP and the related systems.

The table below shows the interface map.

	Reporting system	EMAP	State data processing system	State data-reporting system	KAÜ	BKSZ
Reporting system		communicates				
EMAP			communicates	communicates	communicates	communicates
State data processing system						
State data reporting system						
KAÜ						
BKSZ						

Table 12: Map of interfaces

The interfaces are described as follows:

- Interface identification data: Name of connecting systems
- Description of the operation of the interface,
- Name of the data sets transmitted via the interface, description of the usage characteristics, and the name of the metric applied to quantity estimations (data set/characteristic/metric)

Interface	**Reporting system - EMAP**
Interface description	It is always the reporting system calling the web services published by the EMAP. Data retrieved from the EMAP (data set/usage parameter/metric): ▶ Event data generated by the employee/on a scheduled basis, or upon user request/per ~0-5 employee, each month. Depending on public reporting systems providing status indicator data to the EMAP ▶ Data of verification algorithms and related events stored on the EMAP for formal and substantive verification/ upon user request / multiple times per reporting ▶ Event data describing the status of reporting by employers/on a scheduled basis or upon user request/per event ▶ Event data of past reporting/ upon user request / on an ad hoc basis Data sent to the EMAP: ▶ Event data of employers/ upon user request/ per business event.

Interface	EMAP - KAÜ
Interface description	In order to identify and authenticate natural persons using systems connected to EMAP, EMAP is linked to the KAÜ's identity verification service when it is justified. The interface is designed according to the specification of the KAÜ. The data required by the KAÜ is provided by the user, depending on the authentication method chosen.

Interface	EMAP - BKSZ
Interface description	The EMAP uses services of the BKSZ to send messages to the administrative specialist IT systems of public data processing bodies in cases where the specialist IT system is capable of receiving data in such manner. The EMAP sends data prescribed by law on behalf of the employee. The interface is designed according to the specification of the BKSZ service. The EMAP sends the following data: ▶ The data of form-based returns generated as a result of form transformation/ after a successful form transformation/ Their number is maximised at the number of currently submitted returns, which decreases to 0 by the end of the transitional period. The interface will be used until the public administration IT systems receiving the data have switched to receiving event-based reporting. Data in a format currently required by the public administration IT systems is received on the interface, therefore technical changes are unnecessary on the part of the recipient. The person of the sender changes, which needs to be manageable on the part of the recipient, where employers switching to event-based reporting also authorise the EMAP to send returns.

Interface	EMAP – Public data processing system
Interface description	EMAP calls the services published on the KKSZB to receive data from the public administration IT systems processing data reported by employers. It retrieves the following data from the public administration IT systems of the public data processing bodies: ▶ Status indicator data/ upon request of the employee or employer/ their number continuously increases, depending on the number of offered status indicators. ▶ It queries status messages related to event-based reporting and the list of errors generated when events are accepted or as a result of official audits. It sends the following data from the public administration IT systems of public data processing bodies: ▶ Event data, if the receiving public administration IT system is already prepared to receive event-based reporting/ after the event has been accepted/ their number is constantly increasing as the transition to event-based reporting progresses.

Interface	Public data processing system – BKSZ
Interface description	The administrative data processing IT system uses the services of the BKSZ to send messages to the employer's storage. This is a currently operating interface – there will be no change. The administrative data processing IT system sends the following data: ▶ Receipts related to the receipt of form-based returns/ upon receipt/ per 3-4 sent returns, which will be reduced to 0 by the end of the transitional period. ▶ Official messages related to reporting (e.g. error messages) / ad hoc / ad hoc The interface will be used for as long as form-based reporting is available.

Interface	EMAP – Public administration IT system for public reporting
Interface description	The EMAP calls the services of the administrative IT system for public reporting published on the KKSZB for retrieval of event data. The administrative IT system for public reporting sends the following data in response to the request of the EMAP: ▶ Event data /on a case-by-case basis / their number constantly increases as the number of reportable event types and the number of specialist IT systems providing event data grow.

4.2.3. EMAP technology architecture

This chapter describes the concept of the technological architecture for the operation of EMAP.

Physical locations

Employers, employers' reporting systems, employees can be anywhere, EMAP should therefore be available from anywhere, without geographical restrictions.

The staff operating the EMAP will only be able to access the system from a fixed location.

The EMAP will be hosted in at least two separate data centres (Government Data Centres or KAK). (Currently, public organisations within the scope of the concept are obliged to use the KAK.)

The connection between the users and the data centre is physically provided by a nationwide access network.

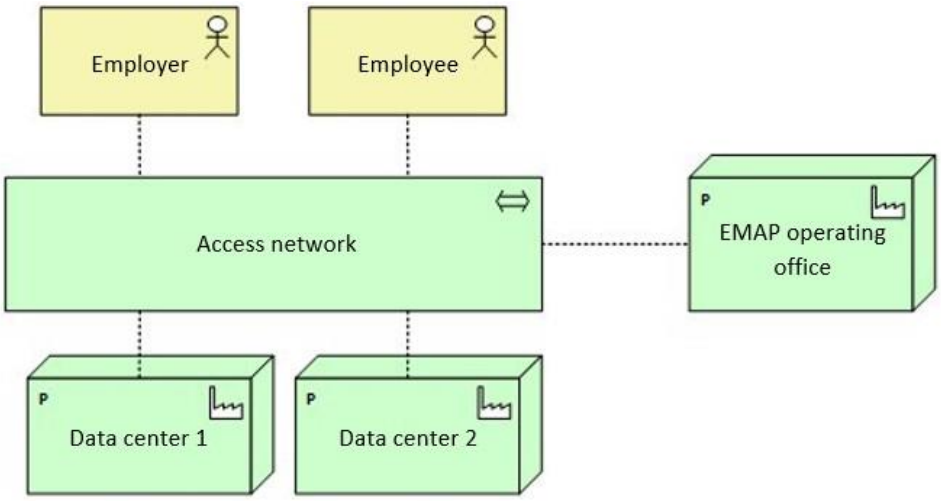

Figure 10: EMAP physical locations

The EMAP operator can provide physical protection only in the data centres. All other sites are regarded as unreliable physical locations for EMAP.

Hardware and system software environment

The hardware and system software environment associated with each architectural component is described below. The table shows the architecture components connected to EMAP, followed by a detailed discussion of EMAP.

Architectural building block	Description of hardware and software environment
Data reporting system	▶ Heterogeneous device portfolio, applications based on a central database developed by market players. Individual IT infrastructure of data providers or payroll service companies.
Computers/Mobile devices	▶ The hardware used by the users can be from any manufacturer and there is no restriction on their installation. ▶ EMAP will indirectly specify requirements for client-side devices in the form of supported software and minimum system requirements.
State data reporting system	▶ Existing reporting systems will be supplemented with servers, database managers and IT network capacity. ▶ The physical environment of the new infrastructure components is the same as the location of public reporting systems at any given time
State data processing system	▶ The current public administration system are complemented by with server providers, database managers, and IT network capacity. ▶ The physical environment of the new infrastructure is the same as the current location of the public administrative systems.
Web / Mobile app	The operating environment used by employed natural persons ▶ conventional, light, medium performance Pcs, notebooks, thin clients, tablets, smartphones.

Architectural building block	Description of hardware and software environment
KEÜSZ/SZEÜSZ (Central Electronic Administration Services / Regulated Electronic Administration Services)	▶ Additional capacity may be required to serve EMAP services, e.g., the large number of KAÜ authentications or an increase in the number of reporting events. ▶ The physical environment does not change.

Table 10: Description of the hardware and software environment for architectural components connecting to EMAP

The EMAP hardware and software environment will be designed to consist of standard components that will be scaled according to the planned transaction numbers:

- Hardware
  - Physical servers for computing capacity
  - Storage system for the physical storage of data
- System software:
  - Virtualization platform
  - Operating System
  - Database management system

The EMAP operation will require additional hardware and software components that are not part of EMAP but must provide capacity to the operating environment.

- Data communication network resources,
- System and security monitoring capacities
- Network security capacities.
- Capacities of security services

The design of the EMAP hardware and software environment will take into account the technology standards of the designated host organisation.

The scaling of the EMAP system and the cost planning described in Chapter 7 were based on the following parameters, using statistical data for 2021-2022 provided by NTCA, NHIF, HST, HCSO or from public sources.

- Number of employers: those providing data to at least of the four authorities in scope (NTCA, NHIF, HST, HSCO). The assumption is that all employers are covered by those providing data to the NTCA. The number of employees is increased by new entities and decreased by ceased ones, thus a relative stability can be assumed. Number of employers submitting at least one data provision form in 2011 to the NTCA: 1,005,617. We assume that one employer equals one EMAP user on average.
- Number of employed persons: The HCSO registered 4.644 million employees in January 2022, with an employment rate of 73.9%. This is group covered by the employers' data provision.
- Reported event data: an average number has been estimated based on currently submitted returns and related events.
- Before submitting event data, EMAP data may be queried several times in connection with a form and content check prior to reporting.

Units of parameter and quantity	Quantity	Web/mobil GUI	EMAP machine interface
Number of EMAP users by number of UI typically used by % distribution			
Employers	1,000,000	30	70
Employees	5,500,000	100	-
Event-based data services			
Reported events/employee/month, average	13		
Number of reported events and their distribution by UI used (reported event/month)	71,500,000	21,450,000	50,050,000
Self-declared event/employee/month	1		
Event data size (in kB)	1		
EMAP data services			
Check query size (in kB)	1		
Event query/employee/month	5		
Event data query per occupied person per month (event/month)	27,500,000	8,250,000	31,192,500
Report queries number/employee/month	1		
Total report queries per month	5,500,000	1,265,700	3,850,000
Report query size (kB)	50		
Number of returns submitted (pcs/month) Excl. average number of returns submitted per month on current form basis	1,500,000		
Return size (size of a return in kB)	10		
Data reporting by public authority specialised systems			
Number of status indicators updated (pcs)	5		
Number of updates of status indicators (per month)	23		
Size of status indicator data (per employee, kB)	0.1		
Events reported by public reporting agent: events/employee/month	1		

Table 11: EMAP scaling parameters

Other aspects taken into account in capacity planning:

- The maximum load is influenced by the fact that 20% of the monthly transaction volume falls on a single day (the day of the reporting deadline) and within an 8-hour interval within which the distribution is considered to be uniform.
- Each business transaction is associated with several technical transactions, e.g. logbook data. Parameter used: 5 technical events.
- Thanks to cloud technology, we plan for a threefold over-allocation of hardware capacity. Hardware capacities and the application need to scale automatically due to the impact of high seasonality (high user activity expected near key data deadlines).

4.3. Comparative evaluation of reviewed technological solutions

In a previous phase of the project, the concept of two potential technological solutions was prepared for implementing the IT services of the EMAP:

- A **system built on centralised data processing and storage** that accepts and stores event data of reporting by employers and makes these accessible to competent authorities. A modern architecture found to be appropriate for similar critical systems has been proposed for the platform built on EMAP centralised data processing. Its two main properties:
    - Deployment of cloud-based platform services in terms of computational capacity, network and data storage, meeting reliability requirements expected and handling high load fluctuations.
    - A microservice-based application architecture running in containers that supports short development cycles and application scalability adapted to needs.
- A **system using distributed ledger (DL) technology** that accepts and stores event data of reporting by employers by use of DL technology in a distributed data storage architecture, and makes these accessible to competent authorities. Main characteristics of distributed ledger technology:
    - Distributed ledger using blockchain technology operating within a private (closed, authorised) network, which would initially have four participants (KSH, MÁK, NAV, NEAK), resulting four nodes.
    - A “proof of authority” consensus mechanism developed for a consortium environment would be applied to validation of event data provision, which offers higher transaction processing speed compared to other consensus mechanisms.

Other services of the EMAP, such as pre-reporting verification services, self-determination, data publication services, form transformation services, would be implemented with technical solutions built on centralised data processingThe following summary analysis summarizes the advantages (+) and disadvantages (-) of the two specific technological solutions presented for central data processing and the distributed ledger along the following aspects:

- **Development aspects:** Evaluation of the factors influencing the implementation of the system and the development process;
- **Architectural aspects:** Evaluation of the factors influencing the structure of the system, the interoperability of its components and the ability to implement business functions;
- **Interoperability:** Evaluation of the factors influencing the interoperability and integration of the system with the related systems;
- **Prerequisites for implementation:** Evaluation of the factors influencing the use of the system;
- **Operation:** Evaluation of the factors influencing the operation and use of the system.

Aspect	Central data processing	Distributed Ledger (DL)
Development aspects	+ Expertise available Proven development methods and tools	+ Uses the traditional development toolkit (Software Development Lifecycle support devices, Continuous Development / Continuous Integration environment, etc.) Supplier-independent solution Reduces the use of IT solutions that are inflexible and difficult to modify - Expert competence is limited Standard software development tools and methods are limited (lack of Software Development Kits, lack of standard frame components e.g. networking, consensus mechanisms)
Architectural aspects	+ It can be built from standard components Reference architecture It is easier to change the technology architecture once the system is in use - The reliability of the system depends on the quality of development and operation Detection-based security (for integrity)	+ Data sharing and authenticity can be achieved with great certainty Prevention-based security - Few industry-class solutions for handling large transaction numbers The design of a specific DLT architecture suitable for a particularly large amount of transactional data requires significant design, prototyping
Interoperability	- The reliability of data exchange is influenced by human factors The exchange of data and the authenticity of data require special technological solutions	+ Reliability of data exchange is a built-in feature of the technology
Prerequisites for implementation	+ There is practice, experience, low risk	- Lack of competence and capacity The applicability of the technology requires more preparation
Operation	+ There is expertise, practice, tools	+ Consensus management provides a high level of operational security (regarding the integrity and retention of data, nodes synchronize and this is maintained permanently). Monitoring can be done with traditional tools and methods. The auditing of the authenticity of the database is simpler. - Lack of competence, capacity and experience to deal with incidents and problems.

Aspect	Central data processing	Distributed Ledger (DL)
Risks	+ Risks are well-known and manageable	Novelty of the technology (pilot handles this) Different IT security model (different knowledge required) Ensuring the right to data erasure

Table 12: Comparison of technological solutions

- From a **development point of view**, the available potential expert competence in terms of quantity and experience is significantly higher in the case of central data processing using mainstream technological solutions than in the case of DL technology. Although there is some training, it is to be expected that, in addition to the general shortage of IT professionals, DL-savvy developers will be even more absent.

  In the case of DL, development frameworks (SDKs) and standards are incomplete, which requires a lot of preparatory development work before the development of real business functions can begin. At the same time, DL technology also uses the traditional development environment and tools.

  Currently few systems built on DL operate in Hungary in a business and State environment, but rapid development of this field is expected (its maturity level, however, will remain low for a long time).

  The shortage of specialists and tools increases the implementation risk (i.e. that the new system will be completed on time, in satisfactory quality, in conformity with objectives), while the novelty of the technology increases operational (security) risks.

  Implementation of customised DLT systems is a more complex task compared to systems built on a traditional database, and selection of the appropriate technical solutions requires more planning, impact analyses, implementation of testing (pilot) solutions.

  The technological solution built on a transparent and shared database enables development of an independent supplier on the elementary level of the architecture.

- In terms of **architecture**, there are a number of reference architectures available for a solution based on central data processing, which significantly reduces the risks associated with the design of the system, both in terms of implementation and operation. The structure and operation of the system is widely known among IT professionals, whereas DL technology is less widespread and unknown to the majority of IT professionals and users. In order to dispel mistrust and gain acceptance of a new technology, it is necessary to inform and train stakeholders.

  One of the outstanding advantages of DLT architecture is when transactions need to be authenticated in a reliable way, as these capabilities are a built-in feature of the technology solution (i.e. data stored in a blockchain is reliably replicated across all nodes). In contrast, for traditional data processing and storage solutions, this is highly dependent on the quality of development and operational practices, as well as on the capabilities of the software used to support the requirements

  DLT enforces secure operation and authentic data storage with the built-in features and tools of the technology in a preventive manner, however, storing the data in blockchain requires significant additional data storage capacity compared to a logically central data storage solution. It is estimated that, considering four nodes, this means a bigger data storage requirement, even compared to a geo-redundant system based on centralised data processing.

Due to the technological peculiarities of DLT systems, a trade-off must be made between decentralization (number of nodes), security (in terms of transaction validation) and performance (number of transactions) because making one of these stronger may be to the detriment of the other two. In the case of EMAP, decentralization is minimal as public authorities are the operators of the DL 'node', therefore the system architecture of the EMAP system based on DLT can provide a high-quality solution in terms of security and performance.

In the case of DL technology, the common view is that the energy demand is high and the processing power of the transactions is low, but regarding to the DL architecture recommended for event-based data reporting system the energy consumption aspects are not relevant, trasaction processing aspects are less relevant, however possible risks should be taken into consideration

Decentralization is not substantial, with only four major, strong public authorities, the number of which will not change much. Thanks to the small number of nodes and the Proof of Authority consensus mechanism chosen, there is a chance that the DLT-based EMAP system will provide adequate performance in terms of security and performance.

Little information is available on working DL solutions that process large numbers of transactions. The experience is that as the number of transactions increases, the load on DL-based systems increases exponentially rather than linearly. For this reason, the use of DL should be preceded by impact analysis and trial implementation.

Given the distinction of the architecture levels, the use of development methods based on standards can be enforced easier during the development process.

- From the point of view of **interoperability**, in the case of a solution based on central data processing, the technological solutions of integrations carry human risks in terms of data authenticity and data exchange reliability, while in the case of DLT solution, data sharing is enforced at the technological level as a basic service. This increases user confidence in the operation of the system.

  The use of standardised DLT platforms will make it easier to ensure interoperability between systems and to perform system upgrades.

- In terms of the prerequisites for **implementation**, the extensive technological experience and competence available in the case of a solution based on central data processing is a clear advantage, as the conditions for implementation and the risks involved are well known. In contrast, DLT has significantly less implementation, operation and development experience as a new, evolving technology segment. There are only a few known DL implementation and even fewer available public information regarding the experiences of the implementation.

  The implementation of a solution based on DL is also more difficult because its acceptance requires more preparatory tasks among decision-makers and other stakeholders, including the legal environment and addressing emerging security and privacy concerns. As with any new technology, it must comply with the practices already known in the current environment and its suitability must be proven in all respects.

- **Operationally,** in terms of the DLT solution, managing distributed registries are a standard feature of the technology so it has superior operational reliability and disaster tolerance ability which the traditional IT data storage and operational management can ensure only with a higher risk.

  In contrast, a solution based on DL must take into account the lack of professionals with operational experience and the greater need for training and support of actors who deal with some DL-specific technology component.

As regards the solution built on DLT, authenticity at data level is based on the technological solution necessitated by the basic technology, therefore audits and verification of data is easier to perform compared to traditional technologies.

When applying DL, it is necessary to take into account the very long data storage periods, which definitely requires the periodic review of applied cryptographic solutions.

The systems need to continuously follow changes in the environment (legal and operational environment, changes in user needs, technological changes), which – based on current experience – will be large in number. There is experience relating to the model based on central data processing using traditional technology, but less experience on DL. The deletion, anonymisation of data in a DL architecture implemented according to an on-chain principle (i.e. substantial data are stored in the blockchain) is a significantly more complex, time-consuming task compared to monolithic data storage.

SWOT analysis

Development of an EMAP system based on central data processing	
Strengths: ▶ Mature architecture and technical solutions ▶ Known implementation and operational risks ▶ Competence, experience available	**Weaknesses:** ▶ Data integrity is ensured by the quality of IT processes, breaches are investigated by detective work ▶ The reliability of data sharing is lower than in the case of the DLT solution
Opportunities: ▶ Managing the reporting of other public authorities (not directly related to employment)	**Threats:** ▶ Resurgence of currently experienced technological problems

Table 13.: SWOT analysis of the central data processing

Use of DLT in development of the EMAP system	
Strengths: ▶ Outstanding storage, sharing of data between nodes in terms of security ▶ The integrated properties of the technology ensure event data integrity, preventive security ▶ A high level of operational security is provided for reporting by employers	**Strengths:** ▶ Outstanding storage, sharing of data between nodes in terms of security ▶ The integrated properties of the technology ensure event data integrity, preventive security ▶ A high level of operational security is provided for reporting by employers
Opportunities: ➡ Automated administrative decision-making ➡ Data repository integration ▶ Managing the reporting of other public authorities (not directly related to employment)	**Opportunities:** ▶ Automated administrative decision-making ▶ Data repository integration ▶ Managing the reporting of other public authorities (not directly related to employment)

Table 14: SWOT analysis of the DLT solution

Conclusion

- The use of DLT is a realistic technology for implementing EMAP, as it provides a technologically enforced, reliable, functional solution to one of the fundamental problems associated with employment (which is credible data sharing and storage between employers, employees and public authorities). This feature of DLT is the most important argument for using DLT, it provides the greatest added value compared to traditional technical solutions.
- The main risk of a DLT-based solution is the relative novelty of the technology and the limited capacity of the workforce with relevant skills available in the already resource-deficient IT labour market.
- Economic actors are typically still experimenting with the technology, solving minor business problems. There are few industry-wide solutions with high transaction performance whose experience has already enriched a common, public knowledge base.
- The novelty of DLT technology and the lack of competent resources pose significant risks to both implementation and operation. This risk will decrease over time as experience is gained and the number of professionals increases. The risk can also be reduced by phased introduction and pilot solutions.
- The two different technological solutions are expected to be comparable in terms of development costs and required software, however, there is a significant difference in hardware costs because DLT requires more data storage capacity due to distributed data storage (data is logically found on all DL nodes, this means five or more odd number of nodes according to the concept).
- DLT is at a disadvantage compared to traditional solutions in terms of information security, as the vulnerabilities of the technical solutions used have not yet been sufficiently analysed due to the novelty of the technology. There is a higher risk that unidentified vulnerabilities will remain in the system.
- The challenges of meeting privacy requirements can be addressed with similar solutions in both architectures.

DLT is a unique software architecture, where optimal transaction management speed is a major challenge. Owing to their basic structure, however, centralised software architectures are not capable of providing a high level of authenticity and a high standard of data sharing. In summary, the development of EMAP is feasible with both central processing technologies and DLT technology, both of which are realistic options.

Defining the business requirements, preparing the functional specification of the EMAP and planning the implementation project does not require a choice between the two technologies in advance; it will be enough to make the choice when selecting the developer organisation implementing the system.

Summary of proposal for the EMAP technological architecture

Due to potential weaknesses of DL, consideration of applying a hybrid technological architecture model is recommended when developing the EMAP system. The basic logic of the architecture would enable retention of the benefits of DLT and traditional central data processing systems, but would eliminate the given technological drawbacks, and could therefore be an ideal solution for achievement of the goal.

The central element of the architecture model, the central database storing event data, would be developed with a traditional relational central database with encrypted, strong access protection. Blockchain based records storing only the asymmetric hash codes of certain event data will be established in parallel (the original data series cannot be generated after generation of the code). The blockchain records should be developed for each natural person and for the employer dimension. In other words,

blockchain records will be established for each employee and each employer, where only the hash code produced from event data relating to the given person or employer is stored. The hash code generated and validated by the blockchain record is also in each case stored for the event for the event data storage record of the “traditional” database storing event data.

Other components of the architecture correspond to the model planned for the central data processing system.

Although application of DL increases system complexity, but event data sent as part of reporting by employers become retrievable together with data stored in the blockchain, objectively supporting inalterability and authenticity, and publishable vis-à-vis competent institutions and data providers. When applying DL, it is necessary to consider the extent to which independent proof of authenticity, reliable storage of event data sent in the course of reporting by employers.

5. Functional and non-functional specifications

5.1. Functional requirements

Functional requirements aim to define functionality provided by the system to be developed. In this process, in addition to setting out operational and usability requirements it is necessary to cover system links and data, and to define reporting, notification and other technical requirements (e.g. archiving, authorisation management, performance).

It is important to emphasise that during the development and operation of the EMAP system, the set requirements essentially define expectations for three responsible actors

- body responsible for implementation of the EMAP, which is responsible for system design and development on the part of the State;
- operator of the EMAP, responsible for operation of the developed system;
- EMAP suppliers, which, as market or State service providers, or authorities providing services, are responsible for delivering specific sub-components necessary for EMAP operation.

The requirements set out in Chapter 3.2.3 in relation to the reporting process are closely linked to requirements summarised in this chapter.

5.1.1. Business functions

Requirements relating to business functions include requirements applicable to the EMAP, defined in connection with individual business process flows.

ID	Requirement	Description
FKÜ-1	General functional requirements	▶ The events can take on uniform status values from preparation until confirmation of their processing, depending on the given step of the workflow ▶ The list of current selectable events on the user platform should be managed so as to enable parametrisation to ensure that changes relating to regulation are followed as fast and as simple as possible, and expected legal compliance (e.g. changing existing legislation, new legislation) ▶ See Chapter 5.1.2 for requirements relating to formal and substantive verification of data

ID	Requirement	Description
		▶ It is recommended that content of data sets requested from employees is managed in a parametrised manner to ensure that changes affecting regulation are followed as simple as possible ▶ When designing the user interface, the aim is to develop a responsive and accessible interface ▶ A general help function should be provided on the interface to facilitate interpretation of data fields to be filled in
FKÜ-2	Preparation of event data	▶ The system should be prepared for both manual reporting by employers and electronic reporting (machine connection) through a connection implemented with a specific external system, and for data set based uploading, which supports the import of specific formats ▶ The formal and substantive verification rules of data should already be applied with priority during preparation of event data, regardless of the means of data input, to prevent incorrect data input ▶ The system should provide a user interface for manual recording of event data in separate versions for employers and employees ▶ The system should provide a user interface for disposition over employee data. Related permissions can be granted or withdrawn in relation to data sets falling within the scope of selected events. When exercising disposition, it is necessary to ensure that permission extends to both data sent earlier by the employer and data received from official specialist IT systems. ▶ When disposing over user data, it is necessary to ensure that authorisation allows the party actually performing reporting (e.g. specialised payroll enterprise or accountant) to access data necessary for reporting for the purpose of work. If lack of authorisation for a data set prevents reporting of an event, this must be indicated to the employer. ▶ It is necessary to ensure the uploading-attachment of data sets that document given event. When designing the system in detail, however, it is necessary to assess if specific data or data set is accessible from an authentic source through system connections implemented with official specialist IT systems. If yes, it should be assigned preference over attachment of the data set.
FKÜ-3	Initiation of reporting	▶ For reporting it should be possible to select a reportable event from a predetermined list – only from meaningful events related to the given status indicator. ▶ Before the sending of data it is necessary to display all necessary aggregating user interfaces assisting verification before sending. ▶ Before sending of data, it is necessary to display the message requesting confirmation, with which the user certifies authenticity of sent data. ▶ The system should be capable of collecting (waiting for) events before acceptance and of forwarding them in a package after appropriate verification (e.g. substantive data verification of specific event, verification of correlations between events).
FKÜ-4	Management of reporting period of employers	▶ Within the system it is necessary to support employers in ensuring that the set of events sent for the given period is blocked and cannot be subsequently modified.

ID	Requirement	Description
		▶ Blocking may apply to the given employer or given reporting period. ▶ In predetermined cases (e.g. administrative decision) it should be possible for predetermined actors (e.g. authorities) to perform unblocking.
FKÜ-5	Acceptance of event data	▶ For events accepted for processing, it is necessary to display the result of sending, which includes the event's unique identifier. ▶ The algorithm for generating the event identifier must take into account that the generated identifier must refer to the type of event.
FKÜ-6	Retrieval of event data	▶ On the querying user interface, retrievable data should be searchable and displayable according to the privilege level: own data in relation to the employee, own events and data sets in relation to the employer and authorising employees, and those accessible only to the given body in relation to authorities. ▶ A search interface must be provided for querying event data, where filters are used for narrowing the set of searched events (e.g. event type, event identifier, 4 natural data (surname and first name, place of birth, date of birth, mother's name), event processing date, status indicator, display of only incorrect events, display of only events requiring correction). ▶ On the interface displaying search results it should be possible to display aggregates (e.g. list, table, cards), and the screen displaying individual event data can be accessed from here. ▶ On the query interface dedicated to employers, in addition to mandatory data, only data shared with them by way of data disposition are visible. ▶ The query interface dedicated to employers is accessible only after KAÜ identification, where the user's own event data are accessible.
FKÜ-7	Transformation of event data and processing of reporting	▶ Successful acceptance of elementary events necessary for data uploading of the given form is a prerequisite for transformation of event data. ▶ Transformation background processes run automatically. ▶ Transformation background processes are scheduled in three ways: o they are triggered by a specific event (e.g. establishment of employment), o they are adjusted to submission deadlines of specific forms (e.g. ME08), or initiated by the employer (verified that events necessary for generating the form have been recorded). o they are launched by the employer ▶ Transformation logic is performed according to the event catalogue ▶ As a result of the successful completion of transformation, the generated form is sent through the BKSZ to the official storage of relevant authorities included in the report and the electronic storage of employers. ▶ It is necessary to manage data transformation between events and forms in a parametrised manner to ensure that changes affecting regulation are followed as simple as possible.

ID	Requirement	Description
		▶ The technical-logical processing of provided data is performed according to prevailing official practice. ▶ This functionality will be eliminated after the transitional period, once authorities can process event data by native means. ▶ During transformation of event data, a form is generated and the transformation procedure also receives a unique identifier.
FKÜ-8	Modification and deletion of events	▶ An event sent earlier, requiring correction can be modified or deleted with dedicated events. ▶ All events requiring correction must be marked and connected by way of a unique identifier to another event containing actually corrected data. ▶ Both the employer and employee must be notified of the fact of correction and tasks. ▶ When developing the corrective event it is necessary to ensure bidirectional communication, to which the event's status must be adapted (return for correction, sending of corrected data, acceptance or rejection of corrected data). ▶ In relation to modifying events, rules maintainable by parametrisation should manage cases in which the given event and its specific attributes may be modified.

Table 15: Business functional requirements

5.1.2. Data and data verification

ID	Requirement	Description
FKA-1	The system manages and stores data falling within its competence, according to their roles	▶ The duration and method of data storage should be determined according legislation in force. ▶ The system manages and stores the following data sets: ○ statistical data ○ data relating to employment (nature of insurance, start and end of insurance, FEOR number, work schedule etc.) ○ data relating to identification (tax number, tax ID, social security number, name, address etc.) ○ wage data ○ data relating to the tax and contribution base ○ payment data related to incapacity for work ○ payment data related to rehabilitation

ID	Requirement	Description
		▶ During data storage, in addition to the data set noted above, it is necessary to also store the parameters (applied rules) of provided data valid at the time of reporting.
FKA-2	All data managed by the system should be retrievable	▶ Users – based on rights determined by their roles – are able to search data. ▶ In most cases queries are accessible in the form of standard reports; in relation to certain roles, unique queries may be defined on a dedicated interface.
FKA-3	During data input the system performs formal verification; in case of an error, an intelligible error message is shown to the user	▶ In the course data input on the web interface, the system performs necessary formal verification (e.g. incorrect number of characters for the tax ID, empty fields etc.) and an error message is shown on the web interface in case of errors. ▶ In the course of data input with an integrated system, the integrated system should perform necessary formal verification and its own interface should show an error message in case of errors. ▶ Data input cannot be finalised until possible formal errors are corrected.
FKA-4	During data input the system performs substantive verification; in case of an error, an intelligible error message is shown to the user	▶ The set of rules recorded in the system should specify the format in which the relevant authority or body expects data as an event or a traditional return. ▶ In the course data input on the web interface, the system performs necessary substantive verification by direct comparison with the EMAP database and an error message is shown on the web interface in case of errors. ▶ In the course of data input with an integrated system, the integrated system should perform necessary substantive verification (provided by the EMAP as a service) and its own interface shows an error message in case of errors. ▶ Data input cannot be finalised until possible substantive errors are corrected. ▶ Three different forms of substantive verification are supported: o Verification of correlations between event types, where ties to, correlations with earlier events are checked o Verification of specialist IT system data: With support from certain integrated official specialist systems, the system compares data content of events to be reported with data (status indicators) of specialist IT systems through provision of appropriate input data. o Verification in sets of events: Verification between elements of sets of events is necessary for jointly reported events ▶ If a sent event package contains an incorrect event, it is sufficient to modify only this event to the appropriate content – substantive verification in this case is run for the set of events.

ID	Requirement	Description
		▶ In case of an event transformation error, the incorrect event and the affected forms are to be determined according to the unique identifier of the transformation procedure.
FKA-5	Data encryption	▶ Data encryption at database level should be ensured in accordance with Article 32 of the GDPR and relevant sections of the Information Act.
FKA-6	Generation of event data	▶ Event data entering the system are continuously entered into the database after launch of the system, without initial database population.

Table 16: Data functional requirements

5.1.3. System connections

Requirements setting out connections of the new reporting system with external systems cover the following points:

- General requirements (on data accessible through the system connection)
- Connections involved in reporting: interfaces supporting data exchanges between the employer providing data and employee users involved in access to their data
- Connections with official specialist IT systems: interfaces supporting data streams to specialist IT systems
- Optional connections: listing of potential system connections necessary not specifically for the business process, but forward-looking

ID	Requirement	Description
FKR-1	General requirements	▶ Pursuant to Section 150 (1) of Government Decree No. 451/2016 (XII. 19.) on detailed rules of electronic administration, management organisations or organisations managing administrative records are required to provide an automatic information transfer service in relation to certain records via the KKSZB (based on number determined by the government decree): ○ 2. registration of citizens' personal data and addresses; ○ 3. land register; ○ 4. Employment and Public Works Database; ○ 5. record necessary for the performance of tasks of the State employment body; ○ 6. single social register; ○ 7. electronic civil status register; ○ 10. pension insurance register; ○ 11. health insurance register; ○ 16. commercial register; ○ 17. register of civil society organisations; ○ 18. central register of aliens;

ID	Requirement	Description
		○ 19. registration systems managed by the support agency for agriculture and rural development; ○ 21. register of self-employed persons.
FKR-2	System connections supporting reporting	▶ EMAP - KAÜ: full identification of natural persons is necessary on the KAÜ platform, where the user can access the system as administration service by use of the Client Gateway password. ▶ Employer systems - EMAP: it is necessary to establish the technical option of a machine connection with various employer reporting systems also by calling services published by the EMAP (e.g. API, micro service, web service), by way of which it is possible to send data directly to the EMAP from various company management, payroll administration systems.
FKR-3	System connections vis-à-vis official specialist IT systems	▶ EMAP - BKSZ: completed return forms are to be forwarded with use of the secure delivery service provided by the BKSZ to the official electronic storage of the relevant authority. ▶ EMAP - KKSZB: the EMAP uses the KKSZB integration service for bidirectional communication with public administration IT systems. The message must contain a specific HTTP header, but specific data may also be sent in various formats (e.g. SOAP/XML, SOAP/JSON, SOAP with Attachment, SOAP MTOM, XML, JSON, text, binary or other data structure). The message has no data limit; it is only dependent on the agreement between the EMAP and the service. The establishment of a direct connection with the public administration IT system should be explored within the context of exception handling. Example services: KSH data change notification, personal data and address register, 4T query. ▶ EMAP - Central Register (ÖNY): the up-to-date, encrypted and scalable Central Register should primarily be the basis for directly retrieving employee data. Involvement of specialist IT systems is justified only if the searched data are not accessible through the ÖNY. ▶ In relation to system connections established with official specialist IT systems, it is necessary to ensure continuous availability of a bidirectional connection between the EMAP and the given specialist IT system. ▶ For system connections implemented with official specialist IT systems it is necessary to manage the particularities of asynchronous reporting (e.g. data stored in the specialist IT systems are deemed to be authentic, but it is possible that employee data change with event processing already in progress).
FKR-4	Optional connection with other external services	▶ Retrieval of citizens' documents from the primary source ○ Diploma certificate and certificate of good conduct – Criminal Record ○ Driving licence - Licence Register ○ Outcome of combined residence and work procedures – Register of Aliens ▶ By implementation of a connection to a data repository containing citizens' personal data (Eidas certificate), data may be retrieved directly from the data repository, which amounts to fewer queries with the

ID	Requirement	Description
		specialist IT systems in terms of system capacities (e.g. presentation of education certificates for establishing employment) ▶ The European Blockchain Services Infrastructure (EBSI) supports cross-border data exchanges, enabling e.g. access to data of company databases.

Table 17: Functional requirements related to system connections

5.1.4. Notifications

The notification requirements applicable to the system may be classified into the following main categories:

- Operational feedback on the EMAP platform: feedback on user interaction results in the system on the user interface;
- Notifications in the form of application messages or e-mails: notification messages to be forwarded to applications (e.g. mobile app, Client Gateway) outside of the EMAP, but using its data;
- Feedback of official specialist IT systems through system connections: requirements defining notifications ensuring information flow (event and status indicator data) between the EMAP and official specialist IT systems.

ID	Requirement	Description
FKÉ-1	Operational feedback on the EMAP platform	▶ Chapter 5.1.2. sets out requirements relating to formal verification of data. ▶ Upon occurrence of the given elementary event, the employer and employee are to be notified on the dedicated EMAP user interface. ▶ Display of a confirmation message on success of user interaction is necessary in each case, e.g. data backups for preparation of data, import from the employer's own system, launch of official correction request. ▶ For all manual reporting by employers or employees, it is necessary to display a confirmation message on the fact of recording and sending, e.g. employee disposition over data, sending of employer events. ▶ For employee disposition over data it is necessary to display a confirmation message on data to which the user grants access; in relation to certain events it may be mandatory to grant access to certain data – both the employer and employee must be informed of this through a system prompt. ▶ In relation to employee disposition over data it is necessary to enable the user to determine events and means of communication used for his/her notification. ▶ In relation to data retrieval it is necessary to display a message on success of retrieval, or the cause of unsuccessful retrieval (e.g. employee data retrieval, status indicator data retrieval and result feedback). ▶ It is necessary to display a message on the EMAP user interface on the result of communication with the official specialist IT systems (e.g. confirmation of sending of return to official storage, notification of start and/or result of official specialist IT system data processing).

ID	Requirement	Description
		▶ For an event to be corrected, notification of both parties concerned should be ensured.
FKÉ-2	Notifications in the form of mobile app messages or e-mail	▶ Upon completion of the return form, notification of the employee with mobile app message or e-mail message generated by the Client Gateway. ▶ It is recommended to send notifications through these channels on the occurrence of events requiring user interaction and approaching deadlines (e.g. correction, necessity of authorisation for disposition over employee data). ▶ It is necessary to define the specific scope of events triggering notifications, and notifications to be sent on their sending, acceptance and processing during the detailed development of the system.
FKÉ-3	Feedback by official specialist IT systems through system connections	▶ Communication by official specialist IT systems serving as a basis for generating notifications is performed through established system connections; related requirements are set out in Chapter 5.1.3. ▶ The system needs to be prepared for generating notifications from interconnected system messages received from the official specialist IT systems on the EMAP user interface, through a mobile app and e-mail, and notifications should also be sent to the official specialist IT system on interactions launched from the EMAP. Example events from the view of the EMAP: ○ *Outgoing notifications:* event occurrence, event acceptance, status indicator feedback to employer and employee, confirmation of sending to official gateway, request for supplementation of missing events for generation of the given form, as part of the reporting obligation; ○ *Incoming notifications:* event sending, employee disposition over data; ○ *Bidirectional notifications:* notification of data processing by official specialist IT systems, notification of required corrections. ▶ It is necessary to define the specific scope of events triggering notifications, and notifications to be sent on their sending, acceptance and processing during the detailed development of the system.

Table 18: Functional requirements related to notifications

5.1.5. Reporting and printing

ID	Requirement	Description
FKN-1	The user can access standard reports	▶ Reports relating to official and employment related matters (e.g. NEAK status) are available to the user in both mobile apps and on the web platform.
FKN-2	The user is capable of printing standard reports	▶ The user is capable of printing available standard reports in both the mobile app and on the web platform.

ID	Requirement	Description
FKN-3	Reporting by employers	▶ The employer can re-verify its own reporting activities with various supporting reports (e.g. status data, list of errors, error reporting on processing).

Table 19: Functional requirements related to reporting and printing

5.1.6. Authorisation management and logging

ID	Requirement	Description
FKJ-1	Legal compliance	▶ The authorisation management and logging processes are in accordance with Act L of 2013 on information security and its implementing decree (Decree No. 41/2015 (VII. 15.) BM).
FKJ-2	A named user account is necessary for accessing the system	▶ Named user accounts should be created for human and technical users.
FKJ-3	Named users need privileges for launching transactions within the system	▶ For launching transactions, privileges should be granted to named user accounts created for human and technical users. ▶ It is necessary to set up WRITING, READING, SEARCH, DELETE basic privileges relating to data managed within the system. ▶ It is necessary to define privileges relating to launching of transactions, e.g. START, APPROVE, CANCEL.
FKJ-4	Within the system, elementary privileges are assigned as part of roles	▶ It is necessary to establish roles for employers, authorities, employees, operators and administrators to ensure efficient management of their privileges by enforcement of the principle of least privilege.
FKJ-5	Incompatible privileges may not be assigned within the system	▶ The SoD (Segregation of duties) matrix must cover the incompatibility of privileges; the system is responsible for enforcing this.
FKJ-6	The system must provide the option of maintaining roles	▶ Upon changes to the legal framework and official / employers' obligations, it should be possible to efficiently modify the privilege system. ▶ It should be possible to modify, delete existing roles and to register new ones. ▶ Individual roles provide querying, modification privileges at data set level, therefore roles created separately for individual authorities, for example, do not display the same data set during querying for all employees.
FKJ-7	The system ensures that unused users are not able to access the system	▶ After certain inactivity, the system blocks the given user account ▶ The inactivity limit varies for individual user groups
FKJ-8	Continuous logging supports system operation	▶ User logins and logouts, and transaction launches are logged. ▶ The start and completion times of scheduled processes, and run results are logged.

ID	Requirement	Description
		▶ The system logs network traffic and modification of logging settings. ▶ The system logs key security incidents. ▶ The system separately logs modification of logging settings.
FKJ-9	The system sends an alarm to operators on all key incidents	▶ The system signals log entries made of key security incidents to operators.

Table 20: Functional requirements related to authorization management

5.1.7. Archiving, saving

ID	Requirement	Description
FKM-1	Legal compliance	▶ The archiving process is in accordance with Government Decree No. 466/2017 (XII. 28.).
FKM-2	The system backs up information managed, used by the system, and stored in electronic form	▶ The system performs full and/or incremental backup of information it manages, stored in electronic form according to schedule.
FKM-3	Saved data must be stored in encrypted form	▶ Data must be saved in encrypted form.
FKM-4	The backup and restore procedures are designed to ensure recovery of the system, if necessary, after unforeseeable events	▶ Day-to-day operation must be ensured in case of a disaster, hardware or software failure, human fault.
FKM-5	The backup does not obstruct workflows, and workflows do not obstruct backups	▶ When scheduling, workflows and backup procedures should be taken into account.
FKM-6	Scope of archived data	▶ Precise definition of the scope of data stored and saved.

Table 21: Functional requirements related to archiving

5.1.8. Performance

ID	Requirement	Description
FKP-1	Cloud-based operation	▶ Deployment of government cloud-based platform services in relation to computational capacity, networks and data storage is necessary to meet reliability requirements applicable to the reporting platform. The solution manages high fluctuation in reporting and loads.

ID	Requirement	Description
FKP-2	Scalability	▶ The system should be adapted to (daily, monthly, annually) serving peak load related to use. ▶ The system should be adapted to the national payroll cycle, where it is necessary to aim for establishing optimal capacities. ▶ For the scalability of the system it is necessary to take into account performance control, where it is necessary to regulate the quantity of permitted simultaneous operations. ▶ Serving high-volatility usage is specifically one of the strengths of cloud-based solutions that allow for flexible and fast scaling of capacities, i.e. increasing or decreasing it, depending on the usage. This provides an opportunity to optimize infrastructure costs that can be allocated on-demand.

Table 22: Functional requirements related to performance

5.2. Non-functional requirements

Non-functional requirements aim to also define conditions and environmental criteria of the system to be developed, which are not directly affecting the system's functionality, but play a determining role in its operation and usability.

It is important to emphasise that during the development and operation of the EMAP system, the set requirements essentially define expectations for two responsible actors:

- the EMAP Operator, the body responsible for the design, development and operation of the system on the part of the State and authorities, and the so-called
- EMAP Supplier, which, as market or State service provider, or authorities providing services, is responsible for delivering specific components for EMAP operation.

The security requirements applicable to IT records listed in safety class 5, set out in Chapter 5.2.3., are related to requirements summarised in the present chapter, the former indicating the organisation category responsible for the given security requirement related to the requirements (EMAP Operator / EMAP Supplier).

The non-functional requirements listed below mainly aim to define general rules meaningful for the EMAP supplier(s).

5.2.1. Compliance

ID	Requirement	Description
NFM-1	Legal and regulatory framework	▶ Act CXII of 2011 on informational self-determination and freedom of information ▶ Act CCXXII of 2015 on general rules of electronic administration and fiduciary services ▶ General Data Protection Regulation (GDPR) ▶ Act L of 2013 on the electronic information security of public and local authority bodies (Information Security Act) ▶ Decree No. 41/2015 (VII. 15.) of the Minister of the Interior on requirements relating to technological security and secure information devices and products defined in Act L of 2013 on the electronic information security of State and local authority bodies, and to classification in security classes and security levels
NFM-2	Legal and standard compliance requirements	▶ The system should be designed so as to ensure that its functionality, data content and service capability is fully compliant with relevant Hungarian laws and standards in force.

Table 23: Non-functional requirements related to compliance

5.2.2. Architecture requirements

Infrastructure and architecture requirements

ID	Requirement	Description
NFA-1	Adaptation to the KAK (Government Data Centre) environmental conditions	▶ Conformity with the operating environment provided for implementation of the system is required. ▶ The central development/installation technology should be adapted to the one used for the NISZ (National Infocommunication Service).
NFA-2	Cloud, SaaS, PaaS	The following requirements are also applicable to solutions provided on a cloud basis, as a SaaS or PaaS service: ▶ if data are stored outside of the KAK, these may only be stored within the territory of the European Union, at predetermined locations ▶ any access to data (e.g. data processing, data management) is possible only from within the territory of the European Union, from locations specified in advance ▶ data stored in the system constitute the property of the Authority in the role of Data Manager, which may be freely accessed and downloaded by the Data Manager ▶ rights of the Data Manager to access data of the Authority, their correction, erasure, restriction, objection to data processing, portability and confidentiality may not be breached ▶ the service provider is involved in data protection impact assessments initiated by the Data Manager and it reports any data protection incidents relating to data of the Data Manager without delay ▶ rights of the Data Manager to return data or to destroy data after completion of the service may not be breached, including the requirement of and solution for secure erasure.
NFA-3	Scalability – its cyclical management	▶ When designing the system it is necessary to apply solutions ensuring seasonal (typically monthly cycle) scalability of the system, and satisfactory operation even upon a further increase in the number of planned users and traffic volume.
NFA-4	Scalability – dimensioning	▶ When designing the system it is necessary to ensure that the entire technological architecture is suitable for the appropriate scaling of performance so as to smoothly satisfy additional capacity needs of higher user number cycles determined in the EMAP Introduction Schedule.
NFA-5	Upgradeability, modifiability	With regard to the developed system it is necessary to take into account the criteria of potential modification and extension, as expected functionality may change as a result of changed processes and legislation. ▶ Modifiability means enabled simple modification of the system's existing functionality. ▶ Potential extension means the possibility of easily adapting new functions, processes and related systems to the system.

NFA-6	Fault tolerance	▶ The technology selected for implementation of the EMAP system must support a modular structure enabling fulfilment of strict fault tolerance requirements defined for functions, modules.
NFA-7	High level of availability	▶ The architecture structure should meet availability requirements defined in conformity with the usage characteristics of specific functions, modules.
NFA-8	Isolated environments	▶ The technologies should serve at least 4 environments isolated from each other (Developer, Test, Pre-live, Operation) at the level of the necessary capacity.
NFA-9	Developer environment	▶ It is necessary to establish a developer environment for designing and developing the deliverable system. At least the following solutions, records should be provided for supporting the development process: ▶ Demand management ▶ Development task management ▶ Configuration (code, documentation) management system ▶ Test management ▶ Change management ▶ Release management
NFA-10	Sandbox	It is necessary to establish sandboxes for testing the system. E.g.: ▶ Integration sandbox, Migration sandbox, User acceptance sandbox. ▶ and the above sandbox should support: the performance test, transition test, operation test, security test, disaster test.

Table 24: Non-functional requirements related to infrastructure and architecture

Interfaces

ID	Requirement	Description
NFA-11	Interface technology	▶ The solutions should provide an SOA based interface at their integration points, which can be integrated in an SOA based infrastructure without additional conversion or special development (Webservice, SOAP, REST/API).
NFA-12	Interface monitoring	▶ A platform should be provided for monitoring messages on interfaces. The system should manage unsuccessfully sent messages (e.g. resending of messages automatically or initiated by the user).
NFA-13	Supported data visualisation methods	In communication, preferred methods of data visualisation may be the following: ▶ XML format, ▶ JSON format, ▶ SOAP format.
NFA-14	With application programming interfaces (API)	▶ The structure of the system should enable programmed API access to its services from other systems and expansion of the range of services accessible by API. The technology to be used for accessing such API should be independent from tools used during implementation of the

ID	Requirement	Description
		system, and it should be accessible regardless of the database and programming language. (e.g. Webservice or other XML based technology).

Table 25: Non-functional requirements related to interfaces

Physical access

ID	Requirement	Description
NFA-15	Use of zoning	▶ When designing the system at module level, it is necessary to take into account that the NISZ protects and monitors communication with zoning at the external and key internal boundaries of the system for boundary protection. To this end it is necessary to develop the individual technological layers (load distributor, web application, database, monitoring etc.) and communication between them with separate zones and firewalls.
NFA-16	Management of external network connections	▶ System components may connect to external networks or external electronic information systems only through interfaces monitored with boundary protection tools.

Table 26: Non-functional requirements related to physical access

5.2.3. Security requirements

ID	Requirement	Description
NFB-1	Security principles of development	▶ As regards input fields, protection against known forms of attack (XSS, Injection etc.) should be provided.
NFB-2	Security principles of development	During development, security risks of the following OWASP Top 10 lists should definitely be managed: ▶ OWASP Most Critical Web Application Security Risks ▶ OWASP Mobile Top 10 Risks ▶ OWASP Top 10 Cheat Sheet ▶ OWASP Top 10 Proactive Controls ▶ OWASP Top 10 Mapped to the Web Hacking Incident Database
NFB-3	Business event logging	▶ The data processing activity of Users or procedures acting on behalf of Users (creation, modification, viewing, deletion of data, access to or use of the system's resources and/or services) must be logged.
NFB-4	Logging of security incidents	Security incidents to be logged: ▶ Successful and unsuccessful login attempts, ▶ Creation and deletion of users, ▶ Changes to user privileges, ▶ Creation, deletion, change of roles, ▶ Start, shutdown of software,

ID	Requirement	Description
		▶ Changes to logging subsystem configuration, ▶ Error messages relevant to operation ▶ Messages related to breach of privileges ▶ Viewing, modification (deletion) of log data ▶ Procedures performed with security functions, parameters, data
NFB-5	Categorisation of log data	▶ Log entries should be classified into categories based on their type and/or severity.
NFB-6	Functions for use of log data	For processing of logs it is necessary to provide a platform enabling: ▶ Viewing (selection, filtering, search) and interpretation of logs for authorised Users ▶ Turning logging on and off ▶ Introduction and management of logging rules
NFB-7	Log archiving	▶ The system should enable periodic archiving of logs.
NFB-8	Modification of unlogged data	▶ As a specific requirement of system operation, unlogged data may not be modified.
NFB-9	Blocking of inactive work phase	▶ The system should enable blocking of a work phase – requiring authentication – after inactivity of a certain period. Access to the system should be possible only after repeated identification and authentication.

Table 27: Non-functional requirements related to security

Encryption, communication protection

ID	Requirement	Description
NFB-10	Protection of traffic in public networks	▶ The confidentiality and integrity of traffic in public networks should be protected with cryptographic solutions accepted and supported by the professional community.
NFB-11	Protection of authentication data	▶ Authentication data should be forwarded from the Client to the server-side application through channels with sufficiently strong encryption.
NFB-12	Forwarding of passwords	▶ The password should be sent through a channel encrypted with a hash value generated with a unique bit series.
NFB-13	System protection	▶ The system should protect data against accidental or intentional destruction, modification, damage and disclosure.
NFB-14	Exclusion of unauthorised persons	▶ Requirement to regulate access to the system and exclusion of unauthorized persons from accessing the system.
NFB-15	Continuous, automated updates	▶ When using devices exposed to harmful software and at risk in terms of human intervention, these must be equipped with appropriate protection. Continuous, automated updating of the protection method's database is a requirement.
NFB-16	Security of boundary protection	▶ A boundary protection solution providing an appropriate level of security must be implemented at the system's external connections

ID	Requirement	Description
NFB-17	Vulnerability testing	▶ To meet legal obligations (Decree No. 41/2015 BM, paragraph 3.3.5.3), during introduction and operation it is necessary to conduct vulnerability testing at system and application level; the security of each of basic software and server operating systems installed must be reinforced (hardening)
NFB-18	Defence against attacks	▶ During development, highly critical attention must be paid to defence against at least the following forms of attack: Protection against injection, Protection against overflow, incorrect access control, cryptographic errors, insecure structure, security misconfiguration, A6) Use of vulnerable and not supported components, Identification and authentication errors, Software and data integrity errors, Security logging and monitoring errors, Server-side request falsification
NFB-19	Encryption of appropriate strength	Encryption of appropriate strength is necessary for all communication involving forwarding of authentication or business data: ▶ Only TLSv1.2 and TLSv1.3 is permitted for SSL algorithms, use of TLSv1.1, TLSv1.0, SSLv3 and SSLv2 is prohibited. ▶ Algorithms recommended for asymmetric encryption: RSA, DSA, and elliptic curve cryptography (ECC) solutions (ECDSA, EdDSA) ▶ Algorithm recommended for symmetric encryption: AES ▶ For RSA and DSA, a minimum key length of 2048 bits, minimum 224 bits for ECDSA and EdDSA, and minimum 256 bits for symmetric encryption must be used. ▶ Hash algorithm: An SHA2 algorithm is acceptable with random length; use of SHA1 and MD5 is prohibited

Table 28: Non-functional requirements related to encryption

5.2.4. Operating requirements

ID	Requirement	Description
NFÜ-1	Operator user interface	An operator user interface is necessary for supporting system operation, which may be accessed only with the appropriate operator and administrator privileges, e.g. ▶ Monitoring, configuration of system processes ▶ Manual launch of processing ▶ Configuration of automatic processing ▶ Testing, administration of system resources ▶ Collection and analysis of events, alarms ▶ User administration
NFÜ-2	Release management	▶ Separate installation of updates of system application elements should be possible according to the necessary technological order, separately from each other, following preliminary functional and technological testing.

ID	Requirement	Description
NFÜ-3	Possible installation	▶ Each on-premise component of the delivered application must have a separately scripted installation package. ▶ The installation package must be run free of error, in conformity with the service manual / implementation plan. ▶ The system's installation package must also support reinstallation of the system. In the process, stored data may not be lost; the installation package must provide for possible data storage modifications. ▶ Before installation it is necessary to deliver the complete source code of software related to system development with appropriate comments. Separate developer documentation must be provided for system components providing services by use of an external interface.
NFÜ-4	Identification	▶ Each user must be individually identified; shared accounts are not permitted in the system.
NFÜ-5	Inactivity management	▶ It should be possible to block the identifier (user access) after inactivity of a given (parametrised) duration or on other grounds.
NFÜ-6	Blocking of identifier, unsuccessful login	▶ It should be possible to manage multiple unsuccessful login attempts (of a parametrised number). ○ blocking of attempting IP, or ○ exponentially increasing response times on the login interface, or ○ use of CAPTCHA etc. ▶ It should be possible to send an alarm on the incident to the system administrator and operating staff.
NFÜ-7	Error message management	▶ In case of the system's faulty performance, it should generate a short error page (e.g. maintenance) for the user, which does not contain any (technical) information describing the system or any element thereof, which the potential attacker can exploit. This should also extend to managing errors in business processes.
NFÜ-8	Role-based privilege management	▶ The system should have role-based privilege management. It should be possible to assign the system's functions (one/multiple) to roles (one/multiple).
NFÜ-9	Principle of least privilege	▶ The system should apply the least privilege principle, i.e. it should grant necessary and sufficient access to users only for execution of their assigned tasks.
NFÜ-10	Monitoring component	▶ The system should have a reporting, monitoring and alarm component at management level.
NFÜ-11	Remote management	▶ The system should be designed to support remote management functions to the extent possible.
NFÜ-12	Architecture supporting centralised management	▶ The system architecture should use technologies ensuring that the use and upgrading of functions and services only generate local IT support needs to a minimal extent. To this end it is important that the technology is a standard solution used in the

ID	Requirement	Description
		IT industry, enabling integration with local IT solutions through standard interfaces.
NFÜ-13	Documentation of operational characteristics	▶ With regard to operational characteristics, the operating documentations should define both permitted ranges and those requiring intervention.

Table 29: Non-functional requirements related to operation

5.2.5. Implementation requirements

ID	Requirement	Description
NFI-1	Ergonomics	▶ The appearance and functionality of screens should have a clear and logical structure
NFI-2	User interface language	▶ The entire interface of the system should be available in Hungarian ▶ The system should correctly manage characters used for completion of forms in Hungarian and in languages of all Member States of the European Union in relation to input, display and alphabetical order.
NFI-3	Accessibility	▶ When designing public pages, it is necessary to ensure that people with disabilities can also securely use them. To ensure accessibility to web content and functions to be implemented on the client side during development, it is necessary to apply key elements of the W3C accessibility standard – W3C WCAG standard, AA level. ▶ The public application should enable reading by text-to-speech software used by the blind and visually impaired. ▶ It is necessary to ensure that pages protected by other “real user” verification systems using captcha or webform can also be accessed by blind/visually impaired persons.
NFI-4	Use of logical data input elements	▶ In each case, where this actually supports efficiency, the modern and user-friendly interface should provide aids for accelerating and enhancing the efficiency of data input by users. These include e.g. value selection fields (drop-down lists), offered values for predictive typing, dynamic and environment dependent narrowing of choice. It should be possible to introduce such and similar solutions in relation to all screens, fields and surface control elements, which simplify use of the system.
NFI-5	Input devices	▶ Work by users should be supported with appropriate (with multiple, as the case may be) input devices (at workplaces where these increase efficiency) – e.g. touchscreen, mouse/keyboard. ▶ The user interface should be uniform, and should support a single structural concept, ergonomics, structure and user logic at system level.
NFI-6	Validation of filled content	▶ Full checks of the correctness of filled content, incorrect data should be clearly indicated during filling in.
NFI-7	Feedback on input errors	▶ During recording of data, data input errors should be indicated to the user as efficiently as possible.
NFI-8	Continuous user interaction feedback	▶ The interface should clearly signal if it is expecting data (it is communicating with other components), or it is unable to accept user

ID	Requirement	Description
		intervention for some reason (e.g. the central system is unavailable, the user cannot access data because of lacking privileges).
NFI-9	Integrated help	▶ The system should provide interactive help accessible from the user interface, integrated in the application.
NFI-10	User-friendly user interfaces	▶ Readily comprehensible UX/UI design supporting system usage by users. Employees should be capable of using basic functions available on the web/mobile platform without training.
NFI-11	Testing	▶ During implementation it is necessary to perform the following types of testing for certain system components: ○ Developer test ○ Functional test consisting of the user acceptance test and integration test ○ Regression test (integrated) ○ Performance test ○ Operation test ○ Migration test ○ Vulnerability (penetration) test ○ Disaster test
NFI-12	Source code	▶ The source code of the individually developed product elements, together with notes, should be available with the procedures creating the executable version and full technical documentation.
NFI-13	Source code	▶ The source code of the delivered software products and solutions, together with notes, should be available at all times with the procedures creating the executable version and full technical development documentation, and provided at least before version changes.
NFI-14	Source code	▶ In relation to delivered commercial off-the-shelf (COTS) solution parts, the source code of the solution, together with notes, should be available at all times with the procedures creating the executable version and full technical development documentation, and provided at least before version changes.
NFI-15	Source code	▶ An unrestricted licence should be provided for use of the delivered source codes.
NFI-16	Used software	▶ Each of the software used for EMAP development, necessary for operation should be ○ accessible to the EMAP operator (available for licensing) ○ regularly maintained software (backed up with a supporting organisation)
NFI-17	Adaptive design	▶ The applications running in the mobile platform browser should be developed in conformity with the principle of adaptive design
NFI-18	Application environment	▶ The applications running in the browser should be functional in both an Android + Chrome mobile, and iOS + Safari environment
NFI-19	User identification	▶ User identification and privilege verification is necessary for developed mobile apps

ID	Requirement	Description
NFI-20	Deletion of stored data	▶ Support of remote deletion of data stored in the mobile app is a requirement
NFI-21	Encrypted data storage	▶ The device may only store data if supported with strong encryption algorithms
NFI-22	Documentation language	▶ All documentation must be in the Hungarian language.
NFI-23	Clarity of documentation, guides	▶ The prepared documentation should correspond to the skill level of the targeted users. Information documents and guides prepared for employees in particular should be readily comprehensible.
NFI-24	Unlimited licence	▶ An unlimited licence, unlimited in time and space, must be provided with the developed software elements.

Table 30: Non-functional requirements related to implementation

5.2.6. Data security requirements

ID	Requirement	Description
NFD-1	Anonymisation and pseudonymisation	▶ Anonymisation and pseudonymisation should be possible within the system. (Article 32(1)a) of the GDPR)
NFD-2	Encryption solutions	▶ Encryption solutions should be used in various layers of the system. (Article 32(1)a) of the GDPR)
NFD-3	Continuous confidentiality	▶ Continuous confidentiality must be ensured in the system. (Article 32(1)b) of the GDPR, Section 25/I. * (3)a) of the Information Act)
NFD-4	Protection against unauthorised activities (data media)	▶ Prevention of the unauthorised reading, copying, modification or removal of data media used by the system. (Article 32(1)b) of the GDPR, Section 25/I. * (3)b) of the Information Act)
NFD-5	Protection against unauthorised activities (data processing system)	▶ Prevention of the unauthorised input of personal data and the unauthorised inspection, modification or erasure of stored personal data in the data processing system. (Article 32(1)b) of the GDPR, Section 25/I. * (3)c) of the Information Act)
NFD-6	Unauthorised use (data processing system)	▶ Prevention of the use of automated data processing systems by unauthorised persons using data communication equipment. (Article 32(1)b) of the GDPR, Section 25/I. * (3)d) of the Information Act)
NFD-7	Privilege based access (data processing system)	▶ It is necessary to ensure that persons authorised to use the data processing system have access only to the personal data covered by their access authorisation. (Article 32(1)b) of the GDPR, Section 25/I. * (3)e) of the Information Act)
NFD-8	Verification of data transfer	▶ It is necessary to verify and to be able to establish the recipients to which personal data have been or may be transferred or made available using data communication equipment. (Article 32(1)b) of the GDPR, Section 25/I. * (3)f) of the Information Act)
NFD-9	Re-verification of data transfer	▶ Subsequently it should be possible to check and determine which personal data were entered into the data processing system, by whom and at what time. (Article 32(1)b) of the GDPR, Section 25/I. * (3)g) of the Information Act)
NFD-10	Protection against unauthorised	▶ In the course of transferring personal data it is necessary to prevent their unauthorised access, copying, modification or deletion. (Article 32(1)b) of the GDPR, Section 25/I. * (3)h) of the Information Act)

ID	Requirement	Description
	activities related to data transfer	
NFD-11	Transport of data media	▶ During the transport of data media it is necessary to prevent the unauthorised access, copying, modification or deletion of personal data during transfers of personal / special data. (Article 32(1)b) of the GDPR, Section 25/I. * (3)h) of the Information Act)
NFD-12	System integrity	▶ It is necessary to ensure the continuous integrity of the system used for processing personal data (Article 32(1)b) of GDPR)
NFD-13	Continuous availability	▶ It is necessary to ensure the continuous availability of the system used for processing personal data. (Article 32(1)b) of the GDPR)
NFD-14	Continuous resilience	▶ It is necessary to ensure the continuous resilience of the systems and services used for processing personal data. (Article 32(1)b) of the GDPR)
NFD-15	Restoring on time	▶ It is necessary to ensure the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident. (Article 32 (1) (c) of the GDPR, Section 25/I. * (3) (i) of the Information Act)
NFD-16	Security testing of data processing efficiency	▶ It is necessary to test the means of assessing and evaluating regularly the efficiency of technical and organisational measures taken to guarantee the security of processing. (Article 32 (1) (d) of the GDPR)
NFD-17	Functionality of the data processing system	▶ It is necessary to ensure the functionality of the data processing system, the generation of reports on errors occurring during its operation and to disable modification of stored personal data even by faulty operation of the system. (Section 25/I. * (3) (j) of the Information Act)
NFD-18	Data connectivity	▶ A technical solution must be in place to ensure that, in order to protect the data sets processed electronically in the various registers, the data stored in the registers by the data controller or, in their scope of activity, the data processor, cannot be directly linked and assigned to the data subject, unless permitted by law. (Section 25/I. * (4) of the Information Act)
NFD-19	Logging requirements	▶ It is necessary to ensure that the system complies with legal requirements for logging. (Section 25/F. * (1) of the Information Act)
NFD-20	Scope of personal data	▶ In the automated data processing system of the data controller and data processor it is necessary to record the scope of personal data affected by the data processing procedure. (Section 25/F. * (1) a) of the Information Act)
NFD-21	Purpose of and justification of data processing procedure	▶ In the automated data processing system of the data controller and data processor it is necessary to record the purpose and justification of the data processing procedure. (Section 25/F. * (1) b) of the Information Act)
NFD-22	Time of the data processing procedure	▶ In the automated data processing system of the data controller and data processor it is necessary to record the precise time of the data processing procedure (Section 25/F * (1) c) of the Information Act)
NFD-23	Person performing data processing	▶ In the automated data processing system of the data controller and data processor it is necessary to specify the person performing the data processing procedure (Section 25/F * (1) d) of the Information Act)
NFD-24	Data transfer recipient	▶ In the automated data processing system of the data controller and data processor it is necessary to record the recipient of transferred personal data. (Section 25/F. * (1) e) of the Information Act)
NFD-25	Data minimisation principle	▶ It is necessary to ensure that only data actually needed for data processing are requested. (Article 5(1)(c) of the GDPR)
NFD-26	Principle of storage limitation	▶ It is necessary to ensure that unnecessary and outdated data are deleted or anonymised after a certain period. (Article 5(1)(e) of the GDPR)

Table 31: Non-functional requirements related to data security

6. Development and implementation plan

6.1. International experience in system deployment

When drawing up the development and implementation plan, international experience in implementation of similar reforms should be considered. There are several international examples of event-based transformation of reporting by employers. Among these, the Australian reform is most closely related to the Hungarian project. We discussed the Australian reform in detail in earlier phases of the project; in this chapter we summarise the most relevant conclusions in relation to the project.

- As regards employment related information, the Single Touch Payroll (STP) of Australia is considered to be the most successful example of transition to event-based reporting. The reporting system preceding reform struggled with problems similar to those in Hungary. An event-based reporting system was introduced in response to these, with a significantly smaller scope than in Hungary (reporting of only financial transactions to the tax authority).
- The initial phase of the STP was launched in July 2018; companies with staff of less than 20 persons were exempted from the usage obligation for one year. Currently employers report payroll data (wages and salaries, income tax deductions, pension fund) in real time to the Australian tax authority (ATO), once payments are made through STP compatible software.

  Introduction of the system was preceded by a comprehensive preparation phase; during 12 months a consultation and co-design process was conducted with data subjects in relation to the system's operation. During this process, free and low-cost STP compatible software products were developed in cooperation with payroll software developers, in consideration of the needs of small enterprises. A pilot programme was also implemented with a focus on small enterprises to gain early user experience.
- Although all employers had the option to start event-based reporting on a voluntary basis from 1 July 2017, the Single Touch Payroll (STP) system was introduced in two phases.
    - The first phase focused on employers with 20 or more employees, including public sector bodies (6.2% of Australian employers, employing 55.8% of the Australian workforce). Event-based reporting was mandatory for these companies from 1 July 2018.
    - The second phase focused on employers with less than 20 employees (93.8% of Australian employers, employing 44.2% of the Australian workforce). Event-based reporting was mandatory for these companies from 1 July 2019.
    - Employers had a grace period of 12 months after the official start date of mandatory STP reporting. During this period, companies did not receive any penalties for failing to lodge their reports.
    - Companies could request delay of the launch time on various grounds (e.g. if they had no or low digital capacities or lacked a reliable internet connection). In practice, the majority of employers requested a delay, as most software developers were unable to implement the necessary changes in payroll software. Additionally, the transition from annual

reporting to event-based reporting required significant additional capacities from employers in terms of both working hours and process steps.

- Beyond the delay, employers could also request other concessions. Agricultural employers, for example, tend to operate on a seasonal basis, therefore the ATO permitted them to perform quarterly reporting instead of event-based reporting. This was also progress compared to previous annual reporting.
- Micro enterprises with up to four employees and limited digital capacities could also report on a quarterly basis until 30 June 2021.

A number of important lessons were learned from the Australian reporting system reform.

- The linking of payroll software and reporting improves data quality, reduces the reporting burden and enhances the digital maturity of small enterprises.
- Comprehensive consultation processes can boost acceptance and support of the system.
- Phased introduction and the flexible approach of authorities can significantly facilitate initial adaptation.
- During introduction it is necessary to ensure operation of the previous system in parallel with the event-based reporting system.
- Validation functions and automated calculations can reduce the data reporting burden.

6.2. Transition plan, deployment strategies

Introduction of the new reporting system will bring about major changes over the existing system in terms of both the process and the technological background, affecting both reporting entities and the data processing public authorities.

The volume of the development project justifies an analysis of the benefits and risks associated with the deployment strategies. This chapter discusses these potential strategies.

The "big bang" approach

Introduction of the new system under a "big bang" approach means that the entire system is deployed in a single step, with no differentiation based on criteria.

This is not realistic in relation to the present project, as the volume of development and the degree of change carries significant risk This is borne out by the fact that the Australian Single Touch Payroll (STP) system described in Chapter 6.1, which is much less ambitious in scope both in terms of the forms covered and the authorities involved, the local government opted for a phased introduction, as will be discussed in more detail below.

Phased introduction

Australia decided on phased introduction of reform—supplemented with various concessions—that is significantly more limited in scope than the present project. It would therefore be justified to apply a phased approach in relation to this development project as well.

There are two potential aspects of phasing:

- **In relation to the relevant data providers:** in line with the Australian example, employers can be grouped on the basis of company size, initially into large and medium-sized enterprise. Based on a possible different approach, the level of digitisation determines which companies are required to join the system after its launch. This may be justified by two factors: first, based on the EY-BI research, regardless of company size, 37–40% of enterprises fully outsource the relevant duties,[17] and second, there is no substantial difference between company sizes in terms of digitisation; in all categories, 68–75% of enterprises are mostly or fully digitised.[18] It is therefore not necessarily justified to permit all small enterprises to subsequently join the system; concession may be conditional on the level of digitisation
- **In relation to the relevant forms**: The primary objective of reform is to reduce the administrative burdens of reporting by employers, which can be fully implemented by the new system only through the channelling of all relevant forms. For this reason, the subsequent inclusion of certain forms in the longer term is recommended only in justified cases. This may apply to the group of forms managed by the Hungarian State Treasury, primarily due to the time needed to answer practical questions arising in connection with the e-PELL development project implemented in parallel.

[17] EY-BI (2020), pp. 22–23.
[18] Ibid., p. 42.

The grace period provided at the launch of the system—similarly to the Australian example—is an additional aspect of phased introduction. In such a case, in the initial period (e.g. in the first six months after launch), entities required to join the system at launch may decide to delay joining. A similar grace period is recommended for enterprises covered by the second phase. In addition, all employers would have the opportunity to voluntarily join the new reporting system during the transitional period. The reporting agents concerned would then have to use both the old and the new reporting systems in parallel, thus ensuring that the new system meets the reporting needs and reduces the burden..

Phased introduction will therefore offer the following benefits over single-phase introduction:

- The reporting entities' burden of transitioning is lighter, as more sensitive enterprises will only have to join in the second phase, and the grace period also supports timely preparation.
- Phased introduction also makes it easier for public authorities to prevent system faults, as not the entire population is using the system, hence fewer errors are expected.
- There are no substantial differences compared to "big bang" introduction in terms of development costs; development of the system is essential for launching.

Implementation of a pilot phase

Another means of phased introduction is the implementation of a pilot phase. Within this pilot, live testing of the core functionalities of the EMAP can be carried out - for up to ten selected companies (joining on a voluntary basis) - in order to identify possible system deficiencies at this early stage. During the pilot phase, the relevant data providers have to use the old and the new data provision system in parallel, thus making sure that the new system satisfies the data provision needs and reduces the burden of data provision.

The advantages of the pilot phase are:

- minimizing technological and implementation risks;
- faster and cheaper "proof of concept" (only the development of the key functions and the specification of the events affected by the companies are required).

The pilot phase was presented in relation to the timeline and budget planning.

6.3. Time required for preparation and related tasks

Prior to the deployment of the system, a number of preparatory activities is essential for successful implementation. Upon phased introduction of the system, based on expert situation assessment the pilot period can begin from the 4th year. With this approach, deadlines can be met if the following preconditions are met:

- Firm support of the government and senior management of the involved public entities;
- Efficient and flexible project management;
- Start of the development tasks at different times, in parallel with other public procurements.

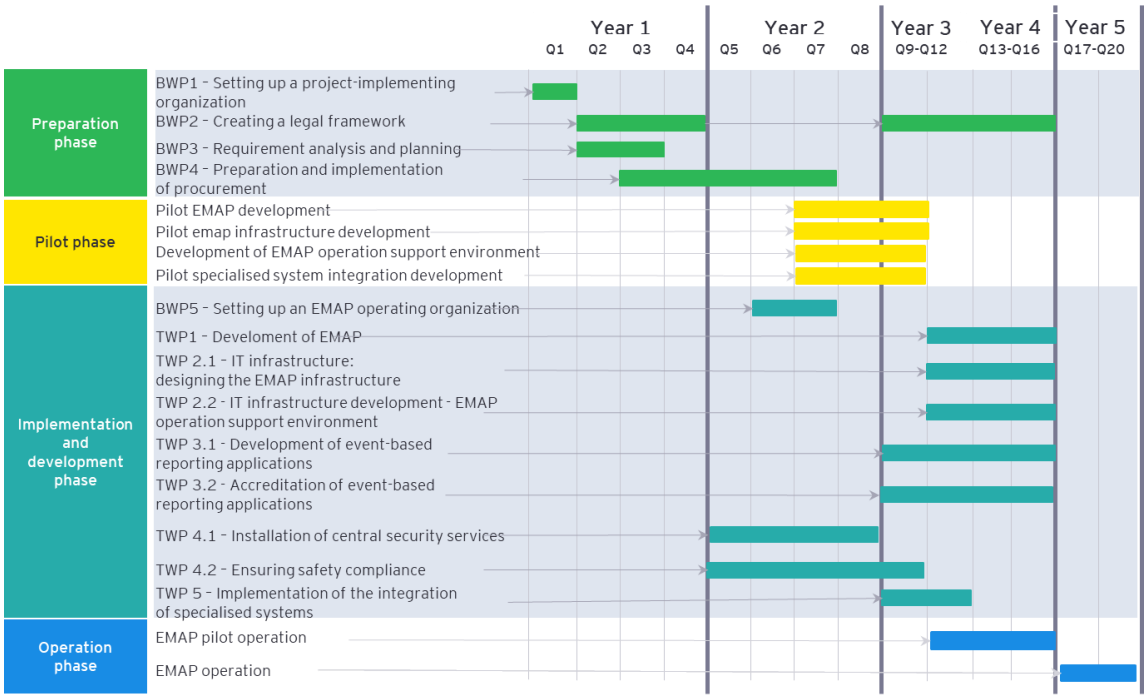

Figure 11: Implementation timetable of the different work packages

6.3.1. Work packages of the preparation phase

Name of work package	**BWP1 – Setup of implementing project organisation**
Objective	Setup of project organisation responsible for implementing the event-based reporting system.
Description	The project is launched with the setup of the project organisation responsible for implementing the EMAP system. It is necessary to appoint the project owner responsible for preparing and implementing the project. The following tasks must be performed as part of setting up the project organisation: ▶ Conclusion of consortium agreement with key actors of the new system (NAV, KSH, NEAK, MÁK); ▶ Definition of appropriate authority and decision-making powers; ▶ Drawing up of the project's operational plan, schedule; ▶ General communication tasks (and determination of communication channels).
Dependencies	Designation of project owner organisation
Implementation criteria	It is necessary to confer appropriate decision-making powers upon the project organisation, with which it is capable of carrying out management and administrative activities during the entire project. It is essential to involve the key actors of implementation (NAV, KSH, NEAK, MÁK) in operation of the consortium.

Name of work package	**BWP2 – Establishment of legal conditions**
Objective	Establishment of conditions for the transition to event-based reporting, and the drafting and entry into force of legislation ensuring operation.
Description	The transition to event-based reporting requires a number of legislative amendments, to be coordinated by the body responsible for implementing the EMAP: ▶ Full identification of necessary legislative amendments; ▶ Preparation and submission of legislative proposals to the relevant public bodies, and coordination of the amendment process.
Dependencies	Dependencies affecting the launch: ▶ BWP1 – Setup of implementing project organisation Dependencies affecting completion: ▶ BWP3 – Assessment of requirements and planning (drafting of detailed business and technical specifications)
Implementation criteria	Identification of legal conditions is a time-consuming task, which can be completed once the precise specification of the EMAP system is available, ensuring that all necessary legal conditions are established.

Name of work package	**BWP2 – Establishment of legal conditions**
	Establishment of the legal framework is a long-term task to be planned as part of the first steps of the project; legislative amendments should be carried out after iterations during development, prior to the live launch of the system.

Name of work package	**BWP3 – Assessment of requirements and planning**
Objective	Drafting of the detailed business and technical specifications of the EMAP system by finalisation of requirements applicable to the system.
Description	Prior to the selection process of the developer organisation it is necessary to draw up the final specifications and list of requirements of the developed system. This requires collection of requirements applicable to the method, with involvement of all relevant bodies of the reporting process, followed by their consolidation and validation. It is necessary to finalise the framework and logical relationships of event-based reporting, on the basis of which development can continue. ▶ Performance of preparatory analyses, planning tasks of the project ▶ Substantive finalisation of event types and drafting of their modification rules ▶ Preparation of the feasibility study of the event-based reporting method ▶ Business specifications: finalisation of the process of the event-based reporting system and of the system functionalities supporting the processes (drafting of list of business requirements). ▶ Technical specifications: Drafting, finalisation of list of non-functional technological requirements, and drafting of target architecture
Dependencies	Dependencies affecting the launch: ▶ BWP1 – Setup of implementing project organisation
Implementation criteria	-

Name of work package	**BWP4 – Preparation and conducting of public procurement**
Objective	Selection of body capable of most efficiently implementing the development project based on predetermined criteria.
Description	It is very likely that the body responsible for developing the EMAP will be selected either by official decision or applications. The selected body/bodies are responsible for covering all services of the event-based reporting platform during development. Potential selection process by way of public procurement: ▶ Drawing up of public procurement call (based on specifications drafted earlier) and determination of evaluation criteria for selection; ▶ Receipt and evaluation of supplier offers (and professional demonstrations) based on the determined set of evaluation criteria;

Name of work package	BWP4 – Preparation and conducting of public procurement
	▶ Selection of the body implementing the development project, conducting of negotiations, followed by drafting of the professional content of the supply agreement.
Dependencies	Dependencies affecting the launch: ▶ BWP1 – Setup of implementing project organisation ▶ BWP3 – Assessment of requirements and planning
Implementation criteria	-

Table 32: Work packages of the preparation phase

6.3.2. Work packages of the development and implementation phase

Based on analysis of variations between the initial and target status architectures, one business and eight technological work packages may be defined in the development and implementation phase, which aim to establish or modify capabilities necessary for reforming reporting by employers.

One work package covers a given project or a portfolio of related projects, involving a public procurement procedure, if an external supplier is involved.

Name of work package	BWP5 – Setup of EMAP operating body
Objective	Setup of body responsible for operating the EMAP.
Description	The implementing project organisation is responsible for setting up the EMAP operating body, during which it is necessary to identify stakeholders in operation, and to define their functions and responsibilities. Processes involved in operation will also be developed. ▶ Drawing up, drafting of agreements between bodies involved in operating the EMAP ▶ Maintenance of event catalogue, management of modification requests ▶ Coordination of technical management activities (application, database, infrastructure operation) ▶ Coordination of change management activities in case of demand, either in relation to legislation or the functionality, algorithms of the system
Dependencies	Dependencies affecting the launch: ▶ BWP1 – Setup of implementing project organisation Dependencies affecting completion: ▶ BWP4 – Preparation and conducting of public procurement ▶ TWP1 – EMAP development

Name of work package	**BWP5 – Setup of EMAP operating body**
Implementation criteria	Setup of the operating body is a prerequisite for defining tasks arising during development of the IT infrastructure.

Name of work package	**TWP1 – EMAP development**
Objective	Development of basic functionality of IT solution enabling event-based reporting
Description	The basic functionality of the event-based reporting platform (EMAP) consists of the following services: ▶ Event catalogue management: registration of catalogue of event types supported by the EMAP ▶ Support of event-based reporting: acceptance of event data, and satisfaction of data requests through a machine interface, on mobile and web platforms ▶ Form transformation: generation of current return-based forms and their sending to authorities on behalf of employers until authorities are prepared to receive native event-based reporting ▶ Self-determination: support of employees' option for self-determination for sharing of event data relating to them ▶ Services supporting operation: other technological services necessary for EMAP operation and implemented as part of the EMAP ▶ KAÜ and BKSZ integration: support of form-based reporting until authorities are prepared to receive native event-based reporting
Dependencies	Dependencies affecting the launch: ▶ BWP2 – Establishment of legal conditions ▶ BWP1 – Setup of implementing project organisation Dependencies affecting completion: ▶ BWP2 – Establishment of legal conditions ▶ TWP2 – development of IT infrastructure: necessary capacities are available, adapted to the scheduled expansion of the group of users, organisational and technical conditions for EMAP operation are available ▶ TWP3 – Development of event-based reporting systems: adapted to the scheduled expansion of the group of users, the reporting systems are prepared for event-based reporting and for receiving data from the EMAP. ▶ TWP4 – Establishment of cybersecurity conditions: EMAP cybersecurity protection is implemented, its audit has been completed, it has received official permits necessary for putting into service.
Implementation criteria	Development and introduction of the EMAP should be harmonised with development of employer reporting systems. The transition to event-based reporting may be gradually extended in a breakdown based on different groups of employers.

Name of work package	**TWP 2.1 - IT infrastructure: Development of EMAP infrastructure**
Objective	Procurement and entry into service of IT infrastructure necessary for EMAP operation
Description	The following technological services are necessary for development of the IT infrastructure required directly for operation of the EMAP as application: ▶ Infrastructure services: hardware, system software, storage systems, network and load distribution systems ▶ Platform services: virtualisation systems, database management systems
Dependencies	Dependencies affecting the launch: ▶ BWP1 – Setup of implementing project organisation Dependencies affecting completion: ▶ BWP5 – Setup of EMAP operating body
Implementation criteria	It is necessary to adjust procurement and putting into service of equipment and services to the schedule for introduction of EMAP services and the involvement of reporting businesses to optimise the use of capacities. Procurement strategy criteria: minimisation of surplus capacities, obsolescence and operating tasks.

Name of work package	**TWP 2.2 - Development of IT infrastructure – Establishment of environment supporting EMAP operation**
Objective	Establishment of background technological services necessary for secure operation of the EMAP.
Description	The body operating the EMAP needs to provide support and technological services necessary for ensuring quality, security and legal compliance of the service. Such technological services should at least be the following: ▶ system monitoring services, ▶ operational and security logging utility, ▶ backup infrastructure ▶ service management system (minimum incident management)
Dependencies	Dependencies affecting the launch: ▶ BWP1 – Setup of implementing project organisation ▶ BWP5 – Setup of EMAP operating body Dependencies affecting completion: ▶ TWP 2.1 - IT infrastructure: Development of EMAP infrastructure
Implementation criteria	The setup or at least designation of the EMAP operating body is necessary for determining the precise technical parameters of the work package, as the local technological standards affect the types of obligations to be considered. It is necessary to put into use the services as early as the EMAP development phase to support operation of various developer and test environments.

Name of work package	**TWP 3.1 - Development of event-based reporting applications**
Objective	Development of IT systems supporting event-based reporting by employers.
Description	IT systems used by employers for managing employment related data, and their typically payroll support or HR systems should be prepared for event-based machine reporting and EMAP integration. These systems should be made capable of ▶ generating data of events contained in the event catalogue ▶ using services published in the EMAP
Dependencies	Dependencies affecting the launch: ▶ BWP2 – Establishment of legal conditions ▶ TWP1 – EMAP development Dependencies affecting completion: ▶ TWP1 – EMAP development ▶ TWP3.2 - Accreditation of event-based reporting applications
Implementation criteria	Sufficient time and information should be provided to developer firms for development and to employers for introducing and putting into service the systems. The specifications of EMAP services should be made accessible and conditions for developer support established on time for introduction of EMAP services and adapted to their scope.

Name of work package	**TWP 3.2 - Accreditation of event-based reporting applications**
Objective	Accreditation of the conformity of event-based machine reporting systems capable of EMAP integration.
Description	Accreditation of the reporting system means that the body operating the EMAP verifies and certifies that the system ▶ performs reporting required by law ▶ is in conformity with applicable technical specifications. Accreditation simultaneously serves the interests of employers and the EMAP. It guarantees that the system is capable of meeting requirements of event-based reporting and protects EMAP integrity. The tasks to be performed: ▶ Definition of accreditation requirements, support of developers of reporting systems, publication of developer SDKs and specifications ▶ Development of sandbox in which developers can check conformity of their systems ▶ Establishment of accreditation procedure ▶ Accreditation of event-based reporting systems
Dependencies	Dependencies affecting the launch: ▶ BWP1 – Setup of implementing project organisation ▶ BWP5 – Setup of EMAP operating body Dependencies affecting completion:

Name of work package	**TWP 3.2 - Accreditation of event-based reporting applications**
	▶ TWP1 – EMAP development ▶ TWP3.1 - Development of event-based reporting applications
Implementation criteria	The time required for accreditation should be considered when scheduling transition to event-based reporting.

Name of work package	**TWP 4.1 – Putting into use central security services**
Objective	Implementation of security services supporting the EMAP system and other operating activities.
Description	The body operating the EMAP should put into service security solutions or extend these to the EMAP, which protect against cyber-attacks, and generally also contribute to data security and legal compliance. Such central security services should at least be the following: ▶ Protection against malware, ▶ Network security solutions,
Dependencies	Dependencies affecting the launch: ▶ BWP1 – Setup of implementing project organisation ▶ BWP5 – Setup of EMAP operating body Dependencies affecting completion: ▶ TWP1 – EMAP development
Implementation criteria	The setup or at least designation of the EMAP operating body is necessary for determining the precise technical parameters of the work package, as the local technological standards affect the types of obligations to be considered. It is necessary to put into use the services as early as the EMAP development phase to protect operation of various developer and test environments.

Name of work package	**TWP 4.2 - Assurance of security compliance**
Objective	Independent verification of the security capabilities of the EMAP and body operating the EMAP
Description	The EMAP system will receive the highest security classification due to the quantity and criticality of processed data, the wide range of uses and the significant impact on them. The system will be exposed to a high threat level and be a constant target for attack, therefore security controls at appropriate level should be established and operated to reduce risks. Compliance with security requirements and identification of vulnerabilities should be ensured with independent security checks integrated in the process. Minimum tasks: ▶ Quality control integrated in the development process to ensure information security compliance and risk management

Name of work package	TWP 4.2 - Assurance of security compliance
	▶ Performance of vulnerability tests and source code audits ▶ Administrative authorisation
Dependencies	Dependencies affecting the launch: ▶ BWP1 – Setup of implementing project organisation ▶ BWP5 – Setup of EMAP operating body Dependencies affecting completion: ▶ BWP2 – Establishment of legal framework ▶ TWP1 – EMAP development ▶ TWP 2.1 - IT infrastructure: Development of EMAP infrastructure ▶ TWP 2.2 - Development of IT infrastructure – Establishment of environment supporting EMAP operation ▶ TWP 4.1 – Putting into use central cybersecurity services
Implementation criteria	The security audit should be integrated in the development process to identify system vulnerabilites and cases of non-compliance as early as possible during implementation. Information security compliance should be certified in relation to each milestone.

Name of work package	TWP 5 - Specialist IT system integration implementation
Objective	EMAP users access authentic data by way of integration implemented with public specialist IT systems. Integration with specialist IT systems serves two purposes: ▶ Replacement of reporting by employees to employers, typically on paper, with electronic, authenticated reporting, the sources of which are the specialist IT systems of State bodies. ▶ Substantive verification of reporting by employers based on (status indicator) data from specialist IT systems of State bodies (NAV/MÁK/KSH/NEAK).
Description	Tasks to be performed within the framework of specialist IT system integration: ▶ Implementation of EMAP - public specialist IT system integration o for obtaining event data related to reporting by employers. Reporting within the specialist IT systems – depending on legal requirements – may be automatic or as a response to data requests from the EMAP, for which the employee grants authorisation. o For querying data necessary for substantive verification of reporting ▶ Use of the self-determination function of the EMAP to enable the employee to dispose over data related to him/her requested from an EMAP integrated official specialist IT system, and over the sharing of data with the employer. ▶ Implementation of EMAP services ensuring availability of data accessible within integrated operation ▶ Expansion of the substantive verification functions of reporting by employers with use of data accessible through integrated specialist IT systems.
Dependencies	Dependencies affecting the launch: ▶ BWP1 – Setup of implementing project organisation ▶ BWP5 – Setup of EMAP operating body

Name of work package	TWP 5 - Specialist IT system integration implementation
	▶ BWP3 – Assessment of requirements and planning Dependencies affecting completion: ▶ BWP2 – Establishment of legal framework ▶ TWP1 – EMAP development
Implementation criteria	Implementation of integration is mainly an organisational challenge, therefore planning is crucial. Conditions of successful implementation: ▶ Very precise identification of relevant data sets ▶ Assessment of data processing authorisation defined by law, establishment of conditions ▶ Coordination of procurements of bodies involved in integration Implementation of integration can be phased according to accepted data sets requested during integration, independently of each other. The implementation schedule must be adjusted to the competence of reporting State bodies, the reporting capabilities of their systems, availability of financing, legal conditions and the time required for procurements. Companies developing the reporting systems of employers must also be involved in implementation to be able receive data made available to them from the EMAP. Employees should also be involved in implementation, and informed of the benefits and use of services available to them. Mixed mode of operation – when not all parties use this EMAP functionality – should be managed at both legal and technical level.

Table 33: Work packages of the development and implementation phase

As regards scheduling it is important to note that employment of a public procurement expert and consultant is necessary from the launch of the project to be on the planned public procurement schedule.

The responsible project owner and project organisation should be fully appointed within three months from launch to be on schedule.

7. Costs and savings of the system implementation

7.1. Costs related to the system implementation

This chapter describes the costs associated with developing the EMAP and its associated infrastructure components. Implementation costs have been summarised in periodical breakdown, according to the following categories:

- Cost of project preparation, covering organisational and specification tasks necessary for launching EMAP development:
  - Setup of project organisation;
  - Drafting of legislation (Phase 1);
  - Professional preparation of implementation project (assessment of requirements and planning);
  - Preparation and conducting of public procurement.
- Cost of implementation, which covers organisational and technical tasks necessary for implementing the EMAP as functional solution:
  - Operation of project organisation;
  - Drafting of legislation (Phase 2);
  - Development costs (EMAP development and integration of public reporting, administration IT systems);
  - Hardware costs (hardware equipment necessary only for the EMAP).
- Operating costs, covering costs incurred in the first 2 years from launch of EMAP services:
  - Deployment costs;
  - Cost of support.

The table below shows the entire planned budget :

Budget item	**Cost (gross HUF)**
1. Total cost of project preparation	**607,000,000 Ft**
1.1. Setup of project organisation (preparation phase)	40,000,000 Ft
1.2. Drafting of legislation (Phase 1)	13,000,000 Ft
1.3. Professional preparation of implementation project (assessment of requirements and planning)	257,000,000 Ft
1.4. Preparation and conducting of public procurement	297,000,000 Ft
2. Total cost of implementation phase	**22,387,000,000 Ft**
2.1. Operation of project organisation (implementation phase)	837,000,000 Ft
2.2. Drafting of legislation (Phase 2)	56,000,000 Ft
2.3. Total cost of EMAP pilot phase	***3,588,000,000 Ft***
2.3.1. EMAP development	2,613,000,000 Ft
2.3.2. Development of EMAP infrastructure (including hardware costs)	510,000,000 Ft
2.3.3. Establishment of environment supporting EMAP operation	132,000,000 Ft
2.3.4 Specialist IT system integration implementation	333,000,000 Ft
2.4. Total cost of EMAP development phase	***17,906,000,000 Ft***
2.4.1 EMAP development	10,384,000,000 Ft
2.4.2 Development of EMAP infrastructure (including hardware costs)	2,040,000,000 Ft
2.4.3 Establishment of environment supporting EMAP operation	1,438,000,000 Ft
2.4.4 Accreditation of event-based reporting systems	138,000,000 Ft
2.4.5 Cybersecurity - Central cybersecurity services	1,176,000,000 Ft
2.4.6 Cybersecurity - Security audit	413,000,000 Ft
2.4.7 Specialist IT system integration implementation	2,317,000,000 Ft
Total cost of system deployment (1+2)	**22,994,000,000 Ft**
3. Total cost of operation phase	**5,983,000,000 Ft**
3.1. Deployment cost (1-year cost of expert support related to the pilot phase, including accreditation costs)	3,324,000,000 Ft
3.2. 1-year cost of expert support in the first year after going live (including accreditation costs)	2,659,000,000 Ft
Total budget of the project (1+2+3)	**28,977,000,000 Ft**

Table 37: Estimated budget of the project

The items of the table are detailed below.

7.1.1. Costs of the project preparation phase

Costs of the project preparation phase are accounted for from the time the decision is taken on implementation of the EMAP. The phase contains costs of tasks necessary for launching actual implementation of the EMAP, consisting of the following cost components:

Budget item	**Cost (gross HUF)**
Total cost of project preparation	**607,000,000 Ft**
Setup of project organisation (preparation phase)	40,000,000 Ft
Drafting of legislation (Phase 1)	13,000,000 Ft
Professional preparation of implementation project (assessment of requirements and planning)	257,000,000 Ft
Preparation and conducting of public procurement	297,000,000 Ft

Table 34: Costs of the project preparation phase

- Operation of project organisation (tasks described in BWP1): The project organisation requires employment of experts with various competencies (project manager, financial manager, administrators, public administration specialists, public procurement specialists); a total of 12 FTEs are needed for 12-26 months, depending on the expert tasks.
- Drafting of legislation (BWP2): Legal experts from relevant authorities should be involved, who provide legal expertise for launching the development project in relation to professional preparation. Six expert FTEs are needed for 2-3 months, depending on the expertise tasks.
- Professional preparation of implementation project (assessment of requirements and planning; BWP3): Involvement of specialists in public administration, IT and public administration is necessary for preparing a detailed feasibility study. The greater the detail and accuracy of professional preparation and related financial planning, the lower the implementation risks. Eight expert FTEs are needed for 6 months.
- Preparation and conducting of public procurement (BWP4): Public procurements must be called and conducted in accordance with the selected public procurement strategy. Related cost components:
    - Work fees of public procurement experts and of public administration and IT specialists involved in the public procurement process;
    - Public procurement administrative fee (projected to the amount of procurement) or other fees directly related to public procurement procedures, of an amount determined by the type of procedure.

  Five expert FTEs are needed for 15 months.

7.1.2. Costs of the implementation phase

Costs of the implementation phase are divided into three main parts:

- Costs related to operation of the project organisation and drafting of legislation, related to the entire period of implementation;
- Costs of the EMAP pilot phase, covering implementation costs of the EMAP system with limited functionality and group of users in the initial year of implementation;
- EMAP implementation costs, covering development costs in the 2nd, 3rd and 4th year, during which time functionality necessary for live operation of the system is implemented.

Costs related to operation of the project organisation and drafting of legislation

Budget item	**Cost (gross HUF)**
Operation of project organisation (implementation phase)	837,000,000 Ft
Drafting of legislation (Phase 2)	56,000,000 Ft

Table 35: Costs of the project implementation phase

The estimation of costs is based on assumptions similar to those for project preparation, with the following differences: they relate to a two-year period and a larger project organisation staff adjusted to more tasks.

Costs of the EMAP pilot phase

Budget item	**Cost (gross HUF)**
Total cost of EMAP pilot phase	***3,588,000,000 Ft***
EMAP development	2,613,000,000 Ft
Development of EMAP infrastructure (including hardware costs)	510,000,000 Ft
Establishment of environment supporting EMAP operation	132,000,000 Ft
Specialist IT system integration implementation	333,000,000 Ft

Table 36: Cost of the pilot phase

Main cost components of the EMAP pilot phase:

- EMAP pilot development costs (part of TWP1), covering only IT development costs. Twenty-two developer, tester, legal and public administration expert, engineer and project manager FTEs are required for 12 months.
- Costs of developing the EMAP infrastructure (part of TWP2.1), which are IT infrastructure costs necessary for satisfying needs of the pilot system, equalling 10% of infrastructure costs.

- Establishment of environment supporting EMAP operation (part of TWP2.2), which are IT development costs of background functions, non-functional requirements necessary for operation of the system; its total cost equals 3% of the cost of the implementation phase at a 20-80% ratio of pilot and implementation, respectively.
- Implementation of specialist IT system integration (part of TWP5), including costs on the part of authorities of integrating the pilot system with official specialist IT systems (performance of five integration tasks – HCSO, HST, NTCA, NHIF, reporting body).

The estimated cost of EMAP pilot development only includes the amount of IT development, covering the development of the system supporting event-based reporting and normative for the contractual amount in relation to external development (i.e. gross amount).

Costs of authorities involved in EMAP development are presented under the heading of specialist IT system integration. This includes all costs of development to be implemented in specialist IT systems related to the EMAP to ensure they can be integrated with the EMAP and capable of performing the necessary reporting and data downloading from the moment of system deployment (it does not include, however, additional development of specialist IT systems aimed at maximising system benefits).

When calculating the development costs, we applied the following expert assumptions:

- The development project will be implemented by an external supplier, according to an agile development methodology. During agile development, 24 sprints can be implemented in one year with 2-week sprints.
- Owing to the upgradeable functionality of the system, the calculations indicate the amount projected for such scheduled years of the development project's implementation, where experts' daily rates are between net HUF 160 thousand and HUF 200 thousand, depending on the given competence.
- Development was implemented for each area of development, i.e. in the breakdown of software module groups, with allocation of the following competencies:

Managerial roles	▶ Project manager ▶ Senior software architect ▶ Chief hardware system architect ▶ Senior business analyst ▶ Senior public administration expert ▶ Chief legal expert ▶ Chief developer ▶ Testing manager
General roles	▶ Quality assurance ▶ Head of group ▶ System organiser ▶ Tester ▶ Developer ▶ System engineer

- Calculation of EMAP infrastructure costs allocated to the pilot period is based on the assumption that implementation of the entire system's infrastructure is not necessary – there is a lower capacity demand, so we accounted for 20% of total costs.
- The methodology used in relation to EMAP pilot development was applied for estimating costs of specialist IT system integration.

- The cost component only estimates integration development costs and does not include the cost of upgrading hardware capacities necessary for satisfying EMAP needs.
- The estimation of integration costs is based on integration cost estimates of earlier projects and could not take into account the possible necessity of developing server systems satisfying the EMAP integration needs.

Costs of the EMAP implementation phase

Budget item	Cost (gross HUF)
Total cost of EMAP development phase	***17,906,000,000 Ft***
EMAP development	10,384,000,000 Ft
Development of EMAP infrastructure	2,040,000,000 Ft
Establishment of environment supporting EMAP operation	1,438,000,000 Ft
Accreditation of event-based reporting systems	138,000,000 Ft
Cybersecurity - Central cybersecurity services	1,176,000,000 Ft
Cybersecurity - Security audit	413,000,000 Ft
Specialist IT system integration implementation	2,317,000,000 Ft

Table 37: Cost of the implementation phase

Main cost components of the EMAP implementation phase:

- EMAP development cost (TWP1), only covering IT development costs (details in the table "EMAP development costs per architecture element");
- Costs of designing the EMAP infrastructure (TWP2.1), which are IT infrastructure costs necessary for satisfying needs of the system;
- Implementation of specialist IT system integration (TWP5), including costs on the part of authorities of integration with their specialist IT systems and of connections to be implemented to data providers (performance of five integration tasks);
- Establishment of environment supporting EMAP operation (TWP2.2), including costs necessary for establishing the EMAP operating environment; its total cost equals 3% of the cost of the implementation phase at a 20-80% ratio of pilot and implementation, respectively;
- Accreditation of event-based reporting systems (TWP3.2). Six expert developer, tester, business analyst, legal expert and project manager FTEs are needed for 12 months, depending on the expertise tasks;
- Cybersecurity - Central cybersecurity services (TWP4.1). 7% of EMAP development and hardware costs;
- Cybersecurity - Security audit (TWP4.2). Fourteen expert FTEs are needed for 5 months, depending on the expertise tasks.

The vast majority of EMAP development costs arise on the part of the State; their breakdown per architecture element is contained in the following table:

EMAP architecture element	Gross HUF
EMAP - Event-based reporting platform	1,703,188,533 Ft
EMAP reporting system	860,822,933 Ft
EMAP browser/mobile app	734,233,567 Ft
EMAP event handling system	1,967,941,200 Ft
EMAP form transformation system	1,344,184,933 Ft
EMAP data publishing system	1,031,172,267 Ft
EMAP self-determination system	352,158,300 Ft
Systems supporting EMAP operation	1,136,997,133 Ft
Public reporting systems	286,512,000 Ft
Administrative specialist IT systems	676,668,700 Ft
KEÜSZ/SZEÜSZ	290,017,200 Ft
Total	**10,383,896,767 Ft**

Table 42: EMAP development costs per architecture element

A smaller share of EMAP development costs arise on the part of employers; the reporting systems currently used by them (HR/payroll systems) need to be prepared for cooperation with the EMAP. Estimated costs may change, depending on the complexity of the used system.

EMAP architecture element	HUF (gross)
Data reporting system	336,046,233 Ft

Table 43: Employer-side EMAP development costs

Costs of EMAP infrastructure design

The table below aggregates the estimated costs of the IT infrastructure (hardware equipment, system software and related licences) necessary for certain functions, including costs of the pilot phase.

Functions	Gross HUF
Hardware costs	950,000,000 Ft
Software costs	950,000,000 Ft
Expert costs related to infrastructure development	650,000,000 Ft
Total	**2,550,000,000 Ft**

Table 44: Hardware costs

- The hardware and licence costs significantly depend on the conditions and discounts potentially effected by the beneficiary.

- Hardware capacity and licence needs significantly depend on technologies used by the developer, the professional standard of the system's design and implementation, and the extent to which it is capable of considering the licensing practice of individual software products.
- Licence costs also depend on the number of used open source software.
- The estimate is based on loads and the hardware needs of other administrative specialist IT systems of similar type and size.

The table below shows the main capacities of the required hardware devices and their estimated cost by application environment. The developer (Dev), Test (Test1), User quality assurance (QA) and productive (Prod) environments are listed in the breakdown of functions, because these may have varying hardware needs.

Serial Number	Environment	Function	Example	CPU (pcs)	Memory (GB)	Storage (GB)
1	Dev	Frontend-node	1	2	12	124
2	Dev	Back-end node	2	2	12	248
3	Dev	Database server	1	4	32	664
4	Test1	Frontend-node	2	2	32	328
5	Test1	Back-end node	4	2	32	656
6	Test1	Database server	2	4	64	1,456
7	QA	Frontend-node	2	2	32	328
8	QA	Back-end node	4	2	32	656
9	QA	Adatbázis szerver	2	4	64	10,456
10	Prod	Frontend-node	4	4	64	912
11	Prod	Back-end node	4	8	64	2,448
12	Prod	Database server	4	12	128	24,496
Total				**146**	**1,732**	**42,772**

Table 45: Breakdown of hardware devices by application environment

Accreditation of event-based reporting systems

There are two main cost components:

- Establishment of accreditation conditions:
    - Establishment of technical conditions for accreditation (development task, to be implemented by the developer team in sprints);
    - Drawing up of accreditation methodology (expert task).
- Performance of accreditation tasks, which is a continuous activity in the second phase of the development project, for which 2 FTEs are allocated.

Cybersecurity - Central cybersecurity services

Cost component allocated to upgrading of the central security services of the operating body. 7% of total development costs.

Cybersecurity - Security audit

The security audit has three cost components for which expert capacities should be allocated:

- Vulnerability testing;
- Source code audit;
- Audit of operating procedures.

7.1.3. Costs of the operation phase

The table below details the operating phase, which includes costs of experts and those incurred on the part of authorities in the first and second year following launch of the live environment (e.g. preparation of legislative changes, organisation, project support, testing, legal and public administration experts).

In the initial period of operation, it is necessary for all bodies participating in the consortium to maintain with reduced capacities a team of experts with the listed competencies, involved in the development phase.

Budget item	Cost (gross HUF)
Total cost of operation phase	**5,983,000,000 Ft**
3.1. Deployment cost (1-year cost of expert support related to the pilot phase, including accreditation costs)	3,324,000,000 Ft
3.2. 1-year cost of expert support in the first year after going live (including accreditation costs)	2,659,000,000 Ft

Table 46: Deployment costs

7.2. Savings from the implementation

The reform is expected to generate substantial savings for both employers and public authorities.

- For employers, the main source of savings is the reduced data requirement attributable to eliminated redundancies and the reduction of administrative burdens caused by incorrect reporting through improved data quality ensured by online validation.
- Direct savings for public authorities are attributable to a number of factors: enhanced efficiency of data processing and verification (and as such, of core activity) by public authorities through data elements and reliable data; improved data quality resulting from online validation, resulting in fewer manually managed cases; additional savings generated by improved official services and use of synergies in system development.

These savings were quantified using two approaches:

- **Saved time for employers:** we estimated the necessary future time allocation of companies on the basis of event-based logic, comparing it to the volume of administrative burden available from earlier research.
- **Financial savings:** based on saved time, we quantified financial savings at national economic level and thereby the payback period of development.

We quantified time saved by employers based on the following premise:

Premise	Related values
An earlier research contains data on current time allocation.	The total median annual time allocation per one employee for employment related reporting is 4.42 hours (according to the weighted average of breakdowns based on company size).
We also took into account the time required for subsequent error correction, which was not included in earlier research. This is relevant in terms of reducing subsequent error corrections to a minimum on the basis of the new system's logic.	Based on input data received from authorities, according to conservative expert estimates, we determined the average time required for subsequent error correction to be 3 percent of total allocated time.
We determined the average time for recording an event in the future event-based reporting system of employers (for an integrated system and a platform provided by the EMAP).	Average time for recording an event: ▶ 1.5 minutes for an integrated system ▶ 2 minutes on the EMAP (web/app) platform
We determined the annual average number of events per employer for the future event-based reporting system of employers, in relation to selected types of companies. In relation to the above, the most important thing to consider is that the number of events is predominantly affected by whether the given	Average annual number of events per one employee: ▶ for companies predominantly employing blue-collar employees: 110 ▶ for companies predominantly employing blue-collar employees: 84

Premise	Related values
firm employs mainly white- or blue-collar employees (company size in this regard is irrelevant). For companies with predominantly blue-collar employees, the specific number of events is higher owing partly to the fragmented compensation structure and partly to more interim loss of working time.	
We determined the weight of various potential groups based on segmentation criteria with relevance for the analysis to be able to apply appropriate weighting for calculation at national economic level.	The expert estimate was aimed at determining the relevant number of employers based on three main segmentation criteria: ▶ company size: base values vary ▶ Type of IT system: average time needed to record an event is shorter through an integrated system ▶ predominantly white- or blue-collar employees: within the new system the annual specific quantity of events significantly varies

Table 42: Premises for quantifying time saved by employers

In the analysis we compared current and future time allocation, as follows:

Average time saved at national economic level	
A. Median time allocation of the current system per employee (hours/year)	4.42
B. Extra time allocation per employee resulting from subsequent error correction in the current system (hours/year) - A*0.03	0.13
C. Total time allocation of the current system per employee (hours/year) - A+B	4.55
D. Average time allocation of the new system per employee (hours/year)	2.61
E. Average time savings of the new system at national economic level (%) - 1-D/C	**42.6**

Table 43: Average rate of time savings at national economic level

By way of the reform, the administrative burden of employers will decline by an average rate of 42.6 percent at national economic level as a result of significantly less time needed for reporting in the event-based system. The actual rate varies for each employer, depending on company size (the smaller the employer, the higher the base value, resulting in higher potential savings), the available IT system (higher savings are possible with an integrated system), and the type of employer (companies predominantly with blue-collar employees are expected to register more events).

The cost of returns and reporting in 2018 related to the employer role amounted to HUF 91.87 billion at annual and national economic level – this is the base for financial savings.

- The above 42.6% decrease in the burden, however, only applies to companies not outsourcing reporting (based on earlier research, 51% of companies carry out reporting exclusively with internal resources).[19]
- **Thus the new system generates potential savings of HUF 19.96 billion at annual and national economic level. When accounting for the total development cost of reform (including preparatory activities at a cost of HUF 28.98 billion), expected savings on the part of employers will cover the EMAP development costs in roughly one and a half years.**
- When calculating the payback period, we did not take into account development costs incurred by employers, but these are offset by volume of savings on the part of authorities, which are not quantified either. The payback period, however, will certainly be lengthened by the system development costs of authorities essential in the long term, and phased introduction proposed on account of the deployability risk may also have a negative effect. Due to the above factors, the above rate of return is considered to be an optimistic estimate.

[19] EY-BI (2019), page 22

8. Annexes

8.1. Demonstration of the future system's operation through a case study (Annex 1)

In this chapter, we demonstrate the operation of the event-based reporting system through a case study. The case study is based on events relating to a fictitious private person, who was employed by an organization that operates as social security payment office and also has integrated payroll software.[20]

István Kiss has just returned from his honeymoon and found employment as an IT specialist as of 1 September 2021 at a company with over 100 employees. After joining the company, he indicated that he wished to receive the first marriage benefit. The employer incorrectly submitted the relevant event as if István intended to receive the benefit alone, even though he intended to receive it jointly with his wife.

In the second week István contracted the coronavirus and received sick pay for two weeks. At the end of the month he received his first month's salary. In parallel with his employment, István also accepts translation jobs as a self-employed person. Due to a deadline he had agreed to earlier, he also had to perform translation during his illness. He performs the accounting of self-employed activity without external assistance.

At the end of October, however, the payroll clerk of István's employer noted that she incorrectly recorded István's night allowance for the month of September, therefore she will correct the error within the framework of the payment event for the month of October.

Thus the following events included in reporting occurred in September 2021 in relation to István:

- Establishment of legal relationship
- Application for first marriage benefit
- Modification – first marriage benefit
- Payment of first month's wages
- Deduction of taxes and contributions
- Contractor's withdrawal

The following event was sent in October in relation to the month of September:

- Modification – night allowance

For each reporting event we show the data content reported, the verification algorithms running in relation to the given event and the modification rules relating to the given event.

[20] It is true for all events in the case study that if the employer does not have an integrated payroll system, the event must be started manually via the EMAP web interface/mobile application. If the process is different, we present the difference in relation to the individual events in the case of employers who do not operate as a social security payment office.

(In the examples below, events are marked by codes; the event catalogue in Annex 8.3 contains detailed data on events.)

Event 1: István Kiss finds a job

István begins work (establishes a legal relationship) on 1 September 2021. His employer records the change to the legal relationship before the start of employment in its payroll system, which produces an event (ETID-3-1, "Start of legal relationship").

Within the current system, changes to the legal relationship must also be reported on an event basis (on the T1041 form of the NAV), therefore the only substantive difference in the process is that within the new system, the employer can manage reporting in its payroll system in an integrated manner. It is sufficient to provide 9 pieces of event-based data and an additional 3 identifiers (for which the EMAP will match 2 other identifiers).

Data content of event

The event contains the following data:

- Identification data (the same for all events)
  - István's tax ID
  - István's social security number
  - István's name
  - Employer's tax ID – if the data provider is the employer, the EMAP automatically loads it based on the user profile. If the data provider is a payroll provider (performing the payroll of several employers), it is required to provide the employer's tax number, on the basis of which the EMAP shows the name of the employer (if the payroll clerk has access to data of the employer).
  - Name of employer (matched by the EMAP)
- Event data
  - start of legal relationship (01.09.2021 - T1041 continuation form 13, row 3);
  - legal relationship code (1101 – continuation form 13, row 5);
  - Employment quality code (2208)
  - FEOR code (2910 – continuation form 13, row 6);
  - number of hours (40 – continuation form 13, row 7);
  - contractual gross wage (data not required for the T1041 form, KSH-MÁK);
  - highest level of education (data not required for the T1041 form, KSH);
  - type of employment contract (data not required for the T1041 form, MÁK);
  - place of business (data not required for the T1041 form, KSH);
- Technical data (the same for all events)
  - Event type identifier
  - Date of event (date: year-month) – automatically loaded on the basis of the "start of legal relationship" data field
  - Date of reporting the event (date: year-month-day-hour-minute-second)
  - Unique technical identification code of event (e.g. hash code)

For events relating to establishment of a legal relationship, the employer is required to manually provide all identification data related to employees.

Verification

Before sending, two types of verification are performed – executed within the payroll system in an integrated manner – in relation to the event. First, formal verification ensures that all data fields related to the event are filled in consistently with relevant rules (e.g. use of valid legal relationship code, gross wage in appropriate format). Second, substantive verification guarantees that only valid events are entered into the system in terms of rights, thereby reducing the risk of data provision found to be incorrect by relevant authorities after acceptance.

The following substantive verification is linked to the event of established legal relationship:

- Links to specialist IT system data (verification)
    - SZL specialist IT system verification (of data of private individuals)
    - Entitlement to old age pension?
- Correlation between event types
    - *Such verification is not related to the event*
- Correlations between event types due to logical relationships between form cells
    - *Such verification is not related to the event*

Modifications

The establishment of a legal relationship is a key event, therefore there are separate events for related modifications:

- ETID-3-2: Change / correction of legal relationship – the data provider uses this event both for retroactive modification (correction) and modification after reporting
- ETID-3-5: Cancellation of legal relationship

If the event passes both formal and substantive verification, the event is sent by the employer to the EMAP, which accepts it and provides feedback on acceptance. The EMAP publishes the event and forwards it to the competent authorities (NEAK, NAV, MÁK, KSH). In a transitional period, the employer also completes the related form (T1041) simultaneously, also sending it to the relevant authorities (NAV, NEAK, KSH) in parallel.

The authority then processes the form (the event itself in the long term), and if it detects any errors during currently also applied verification by specialist IT systems, it provides feedback to the employer. If reporting is free of error, the so-called status indicator may subsequently use the employee's basic data (legal relationship status, FEOR code, number of working hours, data of change to legal relationship), which is aimed at filtering invalid events in terms of entitlement. In the case of István Kiss, for example, his employer will not be able to launch payments with a FEOR code other than the FEOR code submitted in relation to the above event (until the employer modifies the FEOR code in the status indicator with a new event – ETID-3-2, "Change / correction of legal relationship").

Some of the submitted data are utilised to meet data requirements of other, currently used forms; it is unnecessary to report these separately as part of related reporting:

- KSH reporting (e.g. FEOR code, legal relationship code);
- MÁK OSAP reporting (e.g. number of employees);
- 08 return of the NAV (e.g. number of hours, FEOR number).

Event 2: István Kiss submits a declaration for the first marriage benefit

After his hiring, upon István's request, his employer submits a declaration on his intention to receive the first marriage benefit. Currently the benefit may be requested by completion of a paper-based declaration ("Declaration on advance tax for effecting the benefit of persons in a first marriage") or online, on the ONYA platform, which has approximately 40 data fields and thirty of these have to be filled in. Owing to the event logic, within the new system the employer issues the declaration

electronically by provision of only 2 (possibly 4) pieces of data (as shown in the list below), in addition to the identification data. Currently the declaration must be issued each year; within the new system, it would be sufficient to issue it once at the start of entitlement.

Data content of event

The employer registers the related event (ETID-5-1, "Declaration of employee – Tax benefit") in the payroll system. The event contains the following data:

- Identification data (the same for all events)
- Event data
    - start of validity;
    - amount of benefit reducing the tax base;
    - data on spouse (tax ID, name)– the EMAP performs matching when the event is sent, on the basis of employee identifiers, with the Electronic Civil Status Register (EAK);[21]
- Technical data (the same for all events)

Verification

The following substantive verification is performed after formal verification.

- Links to specialist IT system data (verification)
    - Is there a spouse?
    - Does the marriage exist on the declared date?
    - Date of marriage – the date of effecting the benefit is not earlier than the start of entitlement specified by law (first month of marriage, at the earliest)
    - The employee is indeed in his/her first marriage
    - The declared amount is legally compliant (not higher)
    - Has the spouse separately already effected the benefit?
- Correlation between event types
    - Is there a legal relationship between the employee and employer?
- Correlations between event types due to logical relationships between form cells
    - *Such verification is not related to the event*

Modifications

Reported data may be modified with modifying events. This may affect the following data content:

- start of validity
- amount of benefit reducing the tax base

The benefit may be cancelled with a dedicated event.

If the verification algorithm does not identify either formal or substantive errors, the event is submitted by the employer to the EMAP. The EMAP publishes the event on an event basis and/or transforms it to the format of the current declaration, and forwards it to the NAV by both methods. The NAV then processes the declaration, and if it detects any errors during verification by specialist IT systems, it provides feedback to the employer.

[21] Data of the Electronic Civil Status Register have been complete only since 1 July 2014, therefore relevant verification options are also limited. Employees are required issue declarations on previous marriages, and the employer manually uploads data.

Event 3: Modification – First marriage benefit

István planned to receive the first marriage benefit jointly with his wife, by splitting the amount, so each of them would be entitled to a benefit of HUF 2,500. The employer of István, however, recorded a benefit of HUF 5,000, i.e. the full amount of the benefit. When István's wife indicated her intention to receive the benefit to her employer, the EMAP verification algorithm did not permit submission of the relevant event, as István had already claimed the entire amount. Thereafter István informs his employer of his intention to receive the benefit on a shared basis. His employer therefore corrects the incorrectly submitted first marriage benefit event with a modifying event.

In the payroll software the employer retroactively overwrites the data content "amount of benefit reducing the tax base" to HUF 2,500, then the software generates the related modifying event.

If the employer does not operate payroll software, it needs to manually search for the unique identifier of the event to be modified. The data content of the modifying event consists only of the unique event identifier, which is entered, and is followed by the window with the event to be modified. Related verification and modification rules are identical to those of the original event.

István Kiss falls ill

István has a fever on the first weekend of September, loses his sense of smell, so he reports sick in the second work week. He can decide on taking out sick leave or to use his possibly remaining days of leave. István decides on taking out sick leave, which he indicates to his employer, who manages relevant reporting within the framework of paying the monthly wage.

Integration of data on incapacity for work in the EESZT

If enabled by the relevant development, István's GP directly registers his incapacity for work within the EESZT (based on the relevant decision, entering code 7 for COVID symptoms). The EESZT contains the initial date, type (hospitalisation or not) of incapacity for work, and the code for incapacity for work. Based on available information, the social security payment office determines István's entitlement to sick pay and launches payment of the incapacity for work disbursement – information contained in the EESZT serves as a status indicator for the payment event.

The new system essentially completely replaces the paper-based declaration on sick pay (except for the marginal case of foreign sick pay documentation), while the social security payment office engaged by the employer can also rely on authentic data, where the EMAP checks whether István did indeed have an incapacity for work during the given period through the EESZT for assessing/determining sick leave/sick pay. This solution retains the option for employees to settle the period of incapacity for work as leave, because upon such relevant request of the employee, the employer launches a basic payment event and there is no verification through the EESZT.

When István regains his capacity to work two weeks later, his GP registers the last day of incapacity for work within the EESZT, and indicates his capacity for work. Within the new reporting system it is not necessary to physically certify incapacity for work; an electronic version thereof is sufficient, which facilitates reduction of reporting burdens for employers.

István Kiss recovers and resumes work

When István regains the capacity for work two weeks later, he informs his employer of resuming work and submits the sick pay document received from the GP.

Event(s) 4: István receives his first month's wage

At the end of the month, István's employer calculates payments due to him under payroll accounting: wages due for time worked, sick pay he is entitled to in connection with his illness, night work allowance, overtime payment and the stand-by fee. The above can be reported by applying different event types of the two events.

Data content of event

In addition to identification data and technical data, the reported events contain the following data:

ETID-1-1: Payments related to private individuals

- In relation to wages due for worked time: ETID-1-1-1: Event type "remuneration for worked time"
  - ETID-1-1-1-1: Basic salary for worked time, legal title of regular wage
    - Gross amount[22]
    - Number of hours
    - Number of days[23]
    - Reference period
    - Date of payment[24]
- In relation to various allowances, supplements: ETID-1-1-2: "Wage supplement" event type
  - ETID-1-1-2-4: Stand-by supplement
    - Gross amount supplement[25]
    - Number of hours
    - Number of days
    - Reference period
    - Date of payment
  - ETID-1-1-2-6: Night supplement
    - Gross amount[26]
    - Number of hours
    - Reference period
    - Date of payment
  - ETID-1-1-2-7: Basis for extraordinary work (overtime)
    - Gross amount[27]
    - Number of hours
    - Reference period
    - Date of payment
  - ETID-1-1-2-8: Wage supplement of extraordinary work (overtime)

[22] HUF 618,182 for István - row 2108M 300., row 2108M 385., row 2108 M 626., row 2108A 30., and for reporting to the KSH

[23] In the payment events, the number of days and hours for quarterly and annual KSH reporting

[24] In payment events, the correct tax and contribution payment obligation may be determined on the basis of the reference period and date of payment.

[25] HUF 9,195 for István - row 2108M 300., row 2108M 385., row 2108M 626., row 2108A 30., and for reporting to the KSH

[26] HUF 6,900 for István, 2108M 300c

[27] HUF 22,727 for István - row 2108M 300., row 2108M 385., row 2108M 626., row 2108A 30., and for reporting to the KSH

- Gross amount supplement[28]
- Percent
- Number of hours
- Reference period
- Date of payment

ETID-2-1 “Paid benefits related to incapacity for work”

- For the period of incapacity for work: ETID-2-1-2: “Amount of sick pay” event type
  - ETID-2-1-2-1: Non-means-tested sick pay
    - 100% Gross daily base
    - Gross amount (this value is automatically calculated by the EMAP based on the 100% gross daily base and the reference period)[29]
    - Date of payment[30]
    - Reference period[31]
    - Percent[32]
    - Incapacity for work code[33] (the EMAP imports data from the EESZT after relevant development)
    - Declaration of capacity for work (the EMAP imports data from the EESZT after relevant development)
    - Hospital (yes/no) (the EMAP imports data from the EESZT after relevant development)
    - Hospital (yes/no) (the EMAP imports data from the EESZT after relevant development)

In case of an accident at work, the social security payment office may request a procedure for modification of the code.

Special case of non-social security payment offices

In case of a non-social security payment office, the process corresponds to the current one; the employer transfers assessment of sick pay and all other cash health insurance benefits, and of accident sick pay to the government offices, and in this case, disbursement is made by the Hungarian State Treasury (Pension Payment Directorate). For this purpose it fills in the employer’s certificate in the ÁNYK (General Form Completion Programme) and submits it.[34]

Since the sick pay document is also needed for the employer’s certificate, the complete elimination thereof is not possible even after the relevant EESZT development – it will still be necessary in electronic form. This would be possible if the MÁK would be able to directly query relevant data from the EMAP for assessment of sick pay, and employers would not be required to keep paper certificates on incapacity for work.

[28] HUF 11,494 for István - row 2108M 300., row 2108M 385., row 2108M 626., row 2108A 30., and for reporting to the KSH

[29] HUF 85,864 for István, row 2108M 300, and for monthly and quarterly MÁK reporting

[30] For determining the correct tax payment obligation

[31] row 2108M 526, for quarterly MÁK reporting

[32] For quarterly MÁK reporting

[33] row 2108M 526, for quarterly MÁK reporting.

[34] The function should be transferred to the ONYA (Online Form Completion Application) to also support phasing out of the ÁNYK.

Verification

The following substantive verification is performed after formal verification.

- Links to specialist IT system data (verification)
    - If data on incapacity for work will be implemented, the reference period is compared to the period of incapacity for work recorded in the EESZT – the start date and final date of the reference period may not be earlier or later than the one recorded by the physician in the EESZT, respectively.
    - The EMAP can also verify the sick pay percentage rate (whether the employee has 2 years of the legal relationship)
- Correlation between event types
    - Is there a legal relationship between the employee and employer?
    - The type of legal relationship and payment of the incapacity for work benefit is compared, as there are rules of exclusion (e.g. sick pay in one's own and a child's right is not possible for a passive legal relationship).
- Correlations between event types due to logical relationships between form cells
    - The payment events must be jointly sent with PIT and social security deduction events for the EMAP to determine deductible contributions.

Modifications

Special modification rules are applicable to payment events.

- If data is overwritten within a given type of event, the originally submitted event may be overwritten with a modifying event.
- If the amount is overwritten for a different event type, the data provider invalidates the original event (annuls it with a modifying event) and submits the new event. Upon submission of a new event, the reference period of the event indicates a modification relating to an earlier period.

Payment events are not immediately sent after filling in, only together with the deducted tax and contribution events. Therefore, after filling in the events, the employer can save these with the "Prepare for sending" button. When the employer would send the deducted taxes and contributions event, the payment events are also sent.

Currently the 08 return of the NAV serves as the form for monthly payroll accounting; a total of 24 pieces of substantive data need to be provided on its various relevant sheets to have the above events reflected in the return. Within the new system, István's employer can perform the above reporting by completing a total of 32 pieces of substantive data of 2 events (38 substantive data fields including deducted taxes and contributions). The moderately rising data requirement is attributable to the fact that firstly, the number of data fields is increased by the related data requirement of additional forms within the event logic, and secondly, the number of fields relating to tax and contribution data decreases, as these are calculated by the EMAP.

The reported events provide the basis of the 08 return; additionally, they can also be used as part of KSH OSAP reporting and MÁK forms (2395, EB21, 1514), therefore reporting based on event logic clearly reduces redundancy and thereby the administrative burdens of reporting entities. Additionally, since the employer is only required to provide the gross wage, and the EMAP calculates the amount of taxes and contributions, the quality of reporting is improved and the volume of incorrect reporting is reduced. As further enhancement of the above benefits, the system filters benefits without a legal basis and the disbursement of parallel benefits.

The new system does not bring about change in terms of schedule; the legal deadlines (typically the 12th following the relevant month) remain in place.

Event 5: Deduction of taxes and contributions

The data provider may report deducted taxes and contributions after recording of payment events. For this purpose, István's employer opens two event types of an event.

Data content of event

ETID-7-1: PIT – Contributions

- In relation to PIT: ETID-7-1-1: PIT event type
    - ETID-7-1-1-1: Deducted PIT legal title
        - Amount of deducted tax from consolidated tax base
        - Reference period
        - Date of deduction
- In relation to other contributions: ETID-7-1-2: Contribution event type
    - ETID-7-1-2-1: Amount of deducted social security contribution (18.5%) legal title
        - Deducted amount
        - Reference period
        - Date of deduction
        - Reason for omission

The employer can verify correctness of tax and contribution deductions it settled during form transformation; in this process, namely, the aggregate deductions it reported ('08 form, "A" worksheet, row 331) can be compared to the amount deductible tax determined by the EMAP ('08 form, "A" worksheet, row 330). Currently the latter value also has to be calculated and provided by the employer, therefore the values in the two rows are identical in practice. Integration of EMAP calculations, however, provides more reliable verification.

Verification

The following substantive verification is performed after formal verification.

- Links to specialist IT system data (verification)
    - *Such verification is not related to the event*
- Correlation between event types
    - Is there a legal relationship between the employee and employer?
    - Did the employer pay tax abroad during the given period? – ETID-5-3-1-16; ETID-5-3-1-23.
- Correlations between event types due to logical relationships between form cells
    - The EMAP checks the correctness of the amount of deducted taxes and contributions on the basis of payment events and possible relevant declarations, entitlements.

Modifications

If the employer modifies a payment event during the month, it is also necessary to separately launch a modifying event in relation to the tax and contribution deductions for the given month.

Event 6: István withdraws income from the enterprise

At the end of the month, István performs reporting in relation to his activity as self-employed person. In relation to the above, within the current system, related reporting involves monthly submission of the 58 form, which contains a total of 145 data fields. Seventy-one of these are substantive data fields (i.e. not serving identification); in István's case, around 25 fields have to be actually filled in. In contrast, within the new system, István can meet reporting requirements with a single event type ("Income from

self-employment") of a single event (ETID-1-1, "Payments related to private individuals"). Within the event type, he needs to apply the legal title "Amount of withdrawn business income or monthly flat rate income". Without payroll software, he performs this on the EMAP.

Data content of event

- Identification data (the same for all events)
- Event data
  - Gross monthly amount[35]
  - Reference period[36]
  - Date of payment[37]
- Technical data (the same for all events)

Verification

The following substantive verification is performed after formal verification.

- Links to specialist IT system data (verification)
  - István is indeed a self-employed person
- Correlation between event types
  - István does indeed have employment of at least 36 hours
- Correlations between event types due to logical relationships between form cells
  - *Such verification is not related to the event*

Modifications

The related modification rules correspond to those for payments (event 3).

As an advantage of the system, data must be reported only (in contrast with the current obligation) if business income is actually withdrawn in the given month. In place of using the framework programme and fully completing a form, in the future it will be sufficient to report a single event, while the system will calculate taxes and contributions, which improves the quality of reporting and reduces the number of incorrectly reported data.

The system, however, needs to manage tax benefits and incapacity for work in relation to multiple employers, so it is effected only for the employer providing relevant data.

The new system does not bring about change in terms of schedule; the legal deadline (typically the 12th following the relevant month) remains in place.

Event 7: Modification

The employer of István notes that it incorrectly reported István's night allowance for the month of September, and it should have reported only HUF 690 instead of HUF 6,900. Since payroll for the month of September is already closed (all relevant payments and the monthly form transformation have been performed – the employer noticed this after 12th of the following month), the error is corrected during reporting for October. István would generally be entitled to a night allowance of HUF 690 in October as well, which is reported by the employer in October. It manages the overpayment in September, however, with a modifying event. Thus, the employer records the difference for the month of September in the modifying event.

[35] HUF 50,000, 2158-01-01 row 1

[36] From 01.09.2021 to 30.09.2021, 2018 C block

[37] Currently it is not necessary to indicate this on a form – it is needed for tax assessment.

8.2. Data requirements of the current reporting system (Annex 2)

Attached as a separate document.

8.3. Data requirements of the future reporting system (event catalogue, Annex 3)

Attached as a separate document.