DOI: 10.17573/cepar.2023.2.06 1.01 Original scientific article

# Trends in the Digitalisation of Public Administrations – In Light of EU Legislation and Domestic Developments[1]

Adrián Fábián
University of Pécs, Hungary
fabian.adrian@ajk.pte.hu,
https://orcid.org/0000-0003-0103-3077

Gergő Kollár
Univercity of Pécs, Hungary
kollar.gergo@ajk.pte.hu,
https://orcid.org/0009-0008-4595-2941

Received: 30. 9. 2023
Revised: 17. 10. 2023
Accepted: 18. 11. 2023
Published: 30. 11. 2023

ABSTRACT

**Purpose**: Regulating the parameters of all types of identity – including its elements, authenticity and authenticator, verifiability, and the verification process – requires particular attention. The most critical element here is most likely its presence in the digital sphere. Our main goal is to examine the proposal to amend the eIDAS[2] Regulation to create a framework for a European digital identity.

**Design/Methodology/Approach**: The paper analyses the topic in terms of Union law and the most recent strategic document of the Hungarian governmental decisionmaker, incorporating pertinent scientific findings. The article evaluates the current situation, highlighting foreseeable and potential impacts of the new legislative developments.

**Findings**: The paper presents both the practices established by the eIDAS Regulation as a starting point and the current status of digitalisation in Hungary (primarily in public administration).

**Practical Implications**: Eventually, we will attempt to identify the expected opportunities and advantages, as well as risks and drawbacks, associated with the nascent trend of digitalization of public administration in the EU and Hungary.

[1] Supported by the Hungarian Ministry of Justice to improve the quality of legal education.

[2] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (henceforth: eIDAS)

**Originality/Value**: Upon establishing a groundwork in this domain, the nature of the amendment and the domestic response (National Digital Citizenship Programme) will be reviewed to assess efforts at both the European and Hungarian levels.

*Keywords:* *data protection, digital identity, eIDAS 2.0, e-government*

*JEL: K24*

## 1 Introduction

Digital identity refers to the mapping of the unique characteristics of natural persons in the digital world and making them identifiable on this basis. Such an identity is created by digitally storing information about a person and then integrating it into an identification scheme to perform its actual functions (De Hert, 2008, pp. 71).

The particular importance of this area is illustrated by its embeddedness in the application domains of various entitlements that are largely inseparable from modern human existence. Personal data are naturally essential for the creation of identity and its subsequent re-identification, moreover their protection and their processing in accordance with (or at least not in conflict with) the will of the individual are declared as a fundamental human right by the highest-level European Union and national legislations.

In this context, it should be highlighted that with the expansion of the technological toolbox, in some cases even so-called biometric data belonging to a special category of data may be processed, thus exposing the real persons behind the digital identity to greater risk. In addition to the protection of personal data – a need for protection that would not have been possible without the processing of personal data – it is necessary to point out the ability of every person to define themselves from birth, a definition that undoubtedly includes the identity of the individual (unique identity [Sullivan, 2016, pp 478.]).

Although the right to identity has not been established as a fundamental right on its own, it can certainly be grasped as a conglomeration of various other rights. For example, Article 8 of the New York Convention on the Rights of the Child is a constituent element of this, which guarantees every child the right to maintain their own identity[3].

The right to informational self-determination stipulated by Article VI of the Fundamental Law of Hungary is also necessary to be mentioned here, which gives individuals control over personal data. Personal rights under Title XI of the Civil Code are to be noted, too, since the Civil Code explicitly states that everyone has the right to freely assert their personality.

[3] It is perhaps not too far-fetched to assume that this right also applies to adults

# 2 Starting point: EIDAS and the situation in Hungary

## 2.1 The eIDAS regulation

The eIDAS Regulation can be identified as a directly applicable and directly enforceable piece of legislation that is automatically incorporated into the domestic law of all Member States. The EU legislator has used a powerful instrument which, in general terms, suggests a high degree of relevance in this area in terms of European economic relations or the protection of European values (Determann, 2021).

One of the objectives of the legislation is to establish a secure framework for electronic interactions (primarily between the state's authorities and citizens of the Union) and to increase trust in electronic transactions (eIDAS (2) recital) (while improving the efficiency of electronic commerce)[4], which was sought to be achieved by regulating electronic identification and introducing trust services ("More secure transactions on the Internet," 2016).

For these purposes, the Regulation firstly lays down the conditions under which Member States acknowledge electronic identification means of natural and legal persons under the notified electronic identification schemes of other Member States, and secondly, it introduces the rules on trust services for electronic transactions. Thirdly, it establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services and website authentication services (eIDAS Article 1).

An important achievement of eIDAS is that it was the first to establish a cross-border electronic identification framework (eID). In terms of its operational mechanism, it did not seek to harmonise national frameworks, but rather the possibility of mutual recognition and acceptance between Member States by establishing a notification procedure. (Schwalm, 2023)

After the report of the Member States, which are voluntarily participating in the procedure, their eID schemes are examined in detail by a group of experts to ensure that they comply with the requirements of the Regulation[5]. As a result of the assessment, the eID framework will be classified into a security level, which can be low, medium, or high security. The importance of this is that mutual recognition is only binding for other participating Member States if the system is classified as great or high security[6]. The Regulation replaced the previous Directive 999/93/EC[7] when it came in force in 2014, but most of its provisions were not made mandatory until 2016.

[4] Electronic signature, electronic stamp, electronic time stamp, electronic registered delivery services and website authentication

[5] With regard to the implementing acts of the European Commission (EU) 2015/1501, EU) 2015/1502 and (EU) 2015/1984

[6] Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) n° 910/2014 as regards establishing a framework for a European Digital Identity (hereinafter: Impact Assessment Report)

[7] Directive on a Community framework for electronic signatures

Before we look at the positive and negative aspects of the regulation, let us not forget that the COVID-19 pandemic has forced both private and public sector actors worldwide to accelerate digitalisation (research suggests that this could mean a global "time leap" of up to 7 years (McKinsey & Company, 2020) . This has led to user demand for a smooth and complete online administration and rapid response from decision makers. (Strategy on Shaping Europe's Digital Future, 2020). For these, a higher-level institutional system for digital identity is clearly indispensable.

Based on the Commission's impact assessment[8], which was conducted in connection with the Regulation's self-established effectiveness review (Impact Assessment Report pp4./figure 1.), the following conclusions can be drawn about the performance of eIDAS.

Table 1. Evaluating of achievements in the fiel of electronic identification

| **Evaluating achievements in the field of electronic identification** |
|---|
| Only a limited number of eIDs have been registered, which limits the coverage of the reported eID scheme to around 59% of the EU population. |
| The acceptance of registered eIDs is limited, both at the Member State and service provider level. |
| At the EU level, interoperability of several eID systems has been achieved. |
| The lack of monitoring and reporting obligations limits access to reliable data on active contacts and the use of registered eIDs. |
| The actual cross-border use of eIDs is very limited, but the increasing number of transactions in some Member States confirms the positive trend in the usage of registered eID schemes since September 2018. |
| Citizen's lack of awareness of eIDAS and private service providers' low usage of registered eIDs are typical |
| The take-up of eIDAS-based eIDs in the private sector has been insufficient. |
| To allow access to online public services, the current scope of eID schemes registered by Member States is too limited and inadequate. |
| The vast majority of demand for eID and remote authentication will remain in the private sector. |
| The limitations of the eIDAS minimum data package (data content of identity) are a serious shortcoming of many EU sectoral legislations for the implementation of eIDAS solutions. |

[8] Article 49 of eIDAS requires the Commission to review the application of the Regulation by 1 July 2020 at the latest and to report to the European Parliament and the Council

| |
|---|
| The requirements initially defined to pass the eIDAS Regulation are still relevant; the repeal of the Regulation would lead to fragmentation and negative consequences in other legislative areas relying on eIDAS. |
| **Evaluating progress in trust services** |
| eIDAS has successfully created legal certainty on liability, burden of proof, legal effect, and the international aspects of trust services, but some issues remain. |
| The availability and utilisation of trust services in the EU have increased since the introduction of the eIDAS Regulation, but there are differences between the Member States and the various trust services. |
| eIDAS has established a strong framework that can be expanded to include the necessary standards and requirements to reduce the current fragmentation of the market, and the different interpretations of supervisory and conformity assessment bodies. |
| Cooperation between supervisory bodies has been formally achieved to enhance the implementation of eIDAS. |
| New trust services for e-archiving have been established to support the requirements for the digitalisation of paper documents and to support portable identity cards. |
| In some areas, different approaches at the national level have an impact on trust and equal conditions for competition. |
| The Regulation provided a common legal framework for the application of trust services, reducing market fragmentation and encouraging the growth of trust services. |

Source: Authors' determination

The above shows that the eIDAS Regulation has made significant progress in many aspects of the digitalisation of the common market, and in many aspects, it is the first of its kind in the world. However, even with the right intention and target setting, it is clear that the regulatory system of the Regulation does not provide the legal and technical conditions necessary for accelerated progress and therefore changes are needed. The most pressing areas (so-called "pain points") are, according to Viky Manaila[9], the following (Ubisecure-podcast, 2022):

- inflexible and exclusively public sector-focused central identification,
- lack of smooth user experience (e.g. no single sign-in),
- lack of control over personal data,
- lack of regulation on the scope and access of data,

[9] Director of Trust Services, Intesi Group

– different levels of / unequal rules for trust service providers across the EU.

## 2.2 The domestic interfaces

There are many requirements – software, hardware, but also social – that can be listed as the background infrastructure for a digital identity to work. There are currently a range of options for accessing basic services online, but their universality and process integration are still lacking. (Schwalm and Alamillo-Domingo, 2022)

Despite this, the Hungarian legislator – in accordance with the eIDAS Regulation – studied the area in detail[10], which resulted in the development of Act CCXXII of 2015 on the General Rules of Electronic Administration and Trust Services (Eüsztv.) and its implementing regulation, Government Decree 451/2016 (XII. 19.) on the detailed rules of electronic administration. One of the main aims of the Act is to provide a framework with a general horizontal approach for bodies and persons subject to e-government to establish this type of business systems and to enable electronic communication (Baranyi, Homoki and Kovács, 2018).

In Hungary, several major advances have taken place across the board on these conditions. These include the regulated eGovernment Services (SZEÜSZ) and the Central eGovernment Services (KEÜSZ) introduced by the Eüsztv., which support public administrative bodies in the digital switchover, and the Central Identification Agent (KAÜ) and the Client Gateway (ÜK), which provide electronic identification of the public, thus fulfilling the basic requirement for eGovernment (Magyarország Mesterséges Intelligencia Stratégiája, 2020).

Closely linked to the KAÜ and ÜK services is the Central Document Authentication Agent (KDÜ), which can provide (by the client or by the agent of the e-administration body) an electronic document with one of the authentication options available in its system, therefore creating a “one-stop-shop” for users.[11]

In addition to the above, the Personalised Administrative Platform (SZÜF) has been created to promote unified administration, allowing customers to manage their cases with different authorities, courts, other bodies and service providers in a single platform, with a common logic and with a common set of tools. (1. (40) of the Eüsztv.)

Currently, there is also a central electronic mail service, but it is not integrated and is available on two separate interfaces. On one side, the user can send letters on the ePaper site (General Electronic Application Form Service), whereas the user can manage replies on tarhely.gov.hu.

The communication is connected to the Centralised Delivery Agent (KKÜ) service, which provides an integrated platform for the channelling and de-

[10] In the framework of the Digital National Development Programme adopted by Government Decision 1162/2014 (III. 25.)

[11] Probably one of the best known representatives of the system, its so-called minimum service is the authentication of documents based on identification, also known as AVDH

livering of paper-based and electronic mail on a single platform (this can be complemented by the Centralised Receiving Agent (KÉÜ), which allows the automated electronic delivery of mail to the bodies that are obliged to use electronic administration).

Digital document and storage services are already available today but in a somewhat fragmented way. An option for the user is the previously mentioned tarhely.gov.hu, which provides a generic, highly limited storing solution. The other operating system is the Electronic Health Service Space (EESZT), which is much more manageable, but only has a limited functional use for health-related procedures.

Electronic payment services can be seen as another area of online administration. There are several fractioned systems (e.g. the NAV payment system), but one system worth highlighting is the Electronic Payment and Settlement System (EFER), which offers the possibility to pay by credit card on the Internet and has significant potential in this area (if further developed) (Nemzeti Digitális Állampolgárság Program, 2022).

An old feature of digitalisation is still present in everyday life, the General Formfiller (ÁNYK) framework, which supports users in the filling of forms. Lastly, the so-called Association Register (ÖR) should be mentioned, which facilitates the communication and exchange of information between public registers without any link between them, and it is a particularly sensitive area from a data protection point of view. Finally, it should be noted that, almost without exception, the National Infocommunication Service Provider Ltd. (NISZ Zrt.) is the service provider for all the systems listed.[12]

All these systems form the pillars of today's electronic public administration, but the KAÜ and ÜK, as digital identity verification services, deserve special mention in this context.

The Central Identification Agent is an identity verification service provided by the Government on a mandatory basis, as defined in the Eüsztv. Its purpose is to ensure the identification of users – natural person customers and natural person employees of public sector bodies – to the different specialised systems, but the service is not provided by the agent itself, just managed.

The basic service provided by the KAÜ consists of providing an authorised specialised system with the identification of a natural person and the resulting identification data (mandatory and optional). The enhanced KAÜ service (KAÜ+) is more than this, as it provides the authorised specialised system with the identification of a natural person and, in addition, other data, attributes and information on the representative powers of that natural person (KAÜ ÁSZF v3.3).

The ÜK is also an electronic identification service provided by the Government, as defined in the Eüsztv. Its task is to identify the natural person to the online service (specialised system) that requests the identification. In terms of

[12] mo.hu, (2023). Information material on e-administration. Online: www.mo.hu

its operation, the user is connected to a database (Client Registration Register, KÜNY), which is the result of a registration process involving the identification of the person, where they can then log in by entering a username and password (meaning re-verifying their identity). The verification of identity is then sent to the specialised system via the KAÜ system (ÜK ÁSZF v2.6).

## 3 The amendment

The overall revision of eIDAS is currently at the proposal stage, but discussions between the Commission, Council and Parliament on the proposal are progressing positively, with the final version expected to be adopted in the third quarter of 2023 (Ubisecure-podcast, 2022).

The proposed legislation is aimed at moving from national to EU level, thereby – in a cross-border manner – ensuring

- access to highly secure and reliable electronic identity solutions,
- trusted and secure digital identity solutions on which both public and private services can rely,
- empowerment of natural and legal persons to use digital identity solutions,
- linking these solutions to different attributes and allowing targeted sharing of identity data limited to the needs of the service used,
- the acceptance of qualified trust services on an equal basis in the EU.[13]

The objectives described above are in line with the Commission Communication of 9 March 2021 entitled “Digital Agenda to 2030: A European way to achieve the Digital Decade”, which set the goal of an EU framework leading to widespread adoption of a trusted, user-controlled identity by 2030, allowing all users to control their online interactions and presence (this is proposed to mean 80% accessibility for EU citizens by 2030 in terms of users (Wiegl et al., 2022). (The reasoning for these changes is given in the Commission’s 2020 Impact Assessment cited above.)

The scope of eIDAS 2.0 is quite broad: it would cover both natural and legal persons, typically online services, but it would also offer solutions for offline situations. It also seeks to tackle a major shortcoming of the previous version, as the area of application extends beyond public administrations to private sector representatives (eIDAS 2.0 Article 1(a)).

With this extensive applicability, the legislator is explicitly aiming at creating a comprehensive digital identity ecosystem, which would result in a fully harmonised EU system (eIDAS 2.0 (2) Recital). An important milestone for a harmonised application is to tackle the issue of technological interoperability. On one hand, this will involve the creation of a common technological toolbox,

[13] Commission proposal COM(2021) 281 final Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the establishment of a European framework for digital identities (hereinafter referred to as eIDAS 2.0), Explanatory Memorandum, point 1.

which will allow all Member States' systems to be used uniformly (Council makes headway, 2022) and will guarantee a mutually decided and maintained level of security.[14]

A key element of the proposal is a specific case of digital identification, the rethinking of electronic signatures and the rules applicable to them. In this regard, a crucial target is to ensure that all EU citizens can sign electronically (as a quasi-fundamental right). A further important requirement is that how the signature is given (the method used) should be independent of the nature of the device. The Regulation essentially requires technology neutrality (Schwalm and Alamillo-Domingo, 2021, pp. 104.), but it also requires that – in response to technological trends – the possibility to sign on all devices, especially mobile devices, should be ensured (Digital Identity for all Europeans, 2020).

One of the main driving forces behind the proposal is to favour user-friendly solutions, thereby explicitly introducing the principle of 'one-stop-shopping', primarily in the operation of European public administrations (Ubisecure-podcast, 2022). Perhaps the most directly linked to this aim is one of the major innovations of the proposal, the creation of a digital data wallet (Digital Wallet).

This is where the European idea of a digital identity would be concentrated and implemented through its functions, as envisioned by eIDAS 2.0, that is a centralised identification and data storage system (authenticated personal data and attributes[15]) and related services. It is important to emphasise that the use of the Digital Wallet will be free to all EU citizens (eIDAS 2.0 Article 6a(6)) but will not be mandatory (eIDAS 2.0 (5) Recital)

- The Digital Wallet would work in a partially identical way to the real one, so it would be able to store digital versions of all the documents of a person, which would allow digital identity verification ("e-ID").
- The wallet would also include a digital mailbox, which would guarantee communication in an organised, transparent, authentic, and secure way (ePost).
- The wallet would also include an electronic document archive, where documents from administrative procedures and mail exchanges would be stored (eDocument Management).
- In addition to the above, the wallet would be accompanied by an e-signature service that could be used to authenticate documents throughout the EU. This would be paired with a time stamp and an e-stamp, the former to ensure authenticity and the latter to provide legal proof of representative status (eSignature).
- Finally, an electronic payment platform would fully complete the integration of the service package, but this would only cover public payment transactions at the moment (ePayment) (eIDAS 2.0 Article 1.)

[14] It should be noted that the cyber defence training of the system is carried out by the European Cyber Security Agency (ENISA) and the certification mechanisms are carried out in accordance with Regulation (EU) No 2019/881

[15] According to eIDAS 2.0 Article 3(42), an attribute is a characteristic, attribute or attribute of a natural or legal person or entity in electronic form

According to the proposals, the Digital Wallet would cover all aspects of life. It could also be used for administrative purposes such as accessing public services, opening a bank account or filing a tax report. But it would also cover everyday, routine activities such as storing medical prescriptions, presenting a digital driving licence, checking in at a hotel or even just confirming age (Digital Identity for all Europeans, 2020).

The Wallet – as currently understood – would be so universal in character that it would be linked to (or even replace the use of) any other profile used on any other online login platform, from a public portal to a social media platform or even an online shop (eIDAS (21) Recital).

Given the above, it is reasonable to assume that the Wallet – and the data content it carries – would gather the online presence of EU citizenship, in other words, the digital identity that has been scattered and found separately in different service providers, into a single entity. In this context, the proposal has a clear objective of ensuring a more complete informational self-determination for all users, while also attempting to make the digital wallet fully compatible with both data protection and data security.

Protecting the de facto 'centralised' digital identities – and the personal data stored in them – that the Wallet will wish to create is proving to be a major challenge. To achieve this the proposal and its accompanying documents set out several safeguards that are aimed at reducing the risks involved. First and foremost, one possible – and perhaps the most important technically speaking –solution to the current inflexibility of the Regulation, the Zero Knowledge Proof (ZKP) (Impact Assessment Report pp. 30) procedure, needs to be mentioned.

This would provide the authentication requester with the necessary information without providing the exact data content. In practice, this would mean that if an online platform asks for verification of the user's age (e.g. whether they are over 16 years old), the system would confirm this without providing the exact age or date of birth.

It is a major aspect that the new version of the Regulation – as drafted in the proposal – will not require linking public and other records, and will explicitly prohibit the combination of data, in order to respect data management principles (eIDAS 2.0 Article 6a(7)).

This expectation meets a need that emerged in the early days of data protection law, namely the separation of public databases. This is still clearly necessary today, as the problem of information overreach (Szabó, 2012) remains, and the new involvement of large technology companies has only complicated the situation further in the 2010s. In order to overcome this, under the proposed system public databases will remain intact and will continue to operate in accordance with the previous procedures. Under the proposal, these will serve as the "background data" that will allow the above-mentioned ZKP identification to be carried out.

According to Romana Jerković[16], the entire system should be built on principles such as “cybersecurity by design” and “privacy by design” (EPRS Policy Podcast, 2023). These are essential elements in today’s data protection environment, as the GDPR explicitly declares an obligation for data controllers to take and implement appropriate organisational and technical measures (Articles 24-25 GDPR) and to maintain a corresponding data management system.

## 4 Changes: effects and consequences

### 4.1 The opportunities and benefits

Based on an examination of the proposal and other documents, it appears that there are a number of positive benefits to be expected from achieving the stated and specific aims. However, in addition to these, there are certain benefits that are less obvious in the current communications, which may be direct or even indirect and can provide significant benefits to EU actors, regardless of their legal status.

Having listed the obvious benefits in advance, there is no doubt that if the plans are successfully carried out, a properly flowing and much more user-friendly system will be developed compared to the former. This can be deduced from its centralised nature and the well-communicated ‘one-stop-shop’ principle. The public and private services available through a central identification platform are expected to eliminate the necessity of endless profile and password management, thus making private and professional life easier and more efficient. Simplification of this process – if successful – could make online services more accessible and available to groups in society who have previously been hindered by complex, fragmented and sometimes inaccessible systems.

Re-regulating electronic signatures and making them available for free can have a significant beneficial impact on e-commerce, helping consumers and businesses to do business easier in the digital space. A less obvious but technology-neutral e-signature capability, which is widely available and based on the same set of rules, could – if implemented – significantly reduce the operational costs and environmental impact of public services and businesses. For example, very long contracts, service specifications, customer and employee information leaflets could be sent and signed in a fully electronic format without the need for printing in the future. This is well complimented by a qualified archiving service (eDocument Management) that can provide reliable and credible long-term storage, which will assist organisations and individuals in fulfilling their document conservation responsibilities.

Perhaps one of the most positive effects of the eIDAS 2.0 Regulation will be on data management practices and the implementation of informational self-determination. Primarily, the role of Digital Wallets can be significant in maintaining – and in many cases regaining – control over data. At present, service

[16] Member of the European Parliament, Rapporteur for the Committee on Industry, Research and Energy

providers (predominantly in the private sector, but not entirely excluding the public sector) expect users to provide – and where appropriate, continue to provide – self-defined data content on various login interfaces and platforms.

To address this, a system of “notice and consent” given in the spirit of user awareness in relation to the previous regulations does not seem sustainable, for the simple reason that it is no longer expected that a person reads through hundreds of pages of informative material on a daily basis, investigate the scope of the data actually processed, make an informed decision on the processing of the data – with the necessary expertise, of course – and communicate this decision to the service provider through a variety of forms and channels (Solove, 2013). A centralised digital identity, if it can successfully put control back in the hands of the individual concerned, could effectively contribute to the restitution – at least in part – of the previous system. If nothing else, it will certainly promote transparency of data-based business practices and accountability of data controllers.

Taking data management further, making central identification available to all actors across borders and on equal terms would simplify the exercise of data subjects’ rights and at the same time make data controllers’ operations more secure. Currently, effective verification of identity and credible declarations both pose serious problems in practice within and outside organisations. The new Regulation would strongly support the identification and statements of individuals in the exercise of their rights. For example, exercising the right to access (a person’s request for a copy of their personal data) can be done simply and risk-free, as the controller can verify the existence of the right to access without excessive data requests.

If the ePost service can be applied in this area, there will also be significant improvement in the secure transmission of data. Finally, there is a rather distant, but still serious consequence of the introduction of eIDAS 2.0. The reorganisation of the different profiles should not only enhance the user experience but also reduce the quasi-monopoly position of service providers – particularly large technology companies. At present, giant companies[17] such as Meta, Google, Microsoft, Amazon, ByteDance and Apple have the autonomy to define the scope of the data they collect and the way it is used on their own platforms.

The data subjects have minimal influence on this process, not only because of the platform’s own data management practices but also because of its position in the market. The profiles created on the platforms of the companies listed above can be accepted as a registration method for a number of ‘smaller’ providers (Impact Assessment Report pp. 8), but this gives the possibility to broaden the profile and link the records of the activities carried out on different platforms. This so-called digital footprint is currently difficult to restrain and practically impossible to eliminate (regardless of the right to erasure (Article 17 GDPR) that the GDPR would otherwise allow). However, the EU’s efforts to address this situation are evident, with more and more recent legislation in the digital legislative wave of recent years – such as the GDPR,

[17] In the terminology of the Digital Markets Act (DMA): Gatekeepers

DSA[18], DMA[19], MI Regulation[20], e-privacy Regulation[21] – clearly aiming at clarifying the situation of these service providers and securing data management practices. eIDAS 2.0 fits well within this line and is likely to prove effective in this regard.

## 4.2 The risks and disadvantages

For all its advantages, there are considerable risks to be identified and serious drawbacks in the event of failure or possible dysfunctionality of a provision of the regulation.

In many cases, previous advantages can easily turn into disadvantages if not properly applied. For example, the 'one-stop shop' system of the central Digital Wallet can lead to abuse in more serious cases and inconvenience in less serious ones. A system failure could lead to the loss of access not only to one platform but to all of them. Thinking this through, as Rob Rooken[22] has noted, the system could also have the potential to influence or even prevent access to certain platforms or services (even if access is currently voluntary). With increased user vulnerability, it is possible that even with the best legislative intentions, the system will not be able to ensure transparency and could even lead to further abuse by creating the appearance of security.

From a technical point of view, difficulties are expected from several sides. One obvious problem may arise if the implementation is simply not right (even if it is due to a lack of interoperability). This may be due to slowness, difficulty of use or other features of the system, but ultimately the important thing is that users are used to a mature and already existing user-friendly infrastructure on social media platforms. In the event of a significant drop in quality (due to the voluntary nature of the use), it is possible that the space will remain under-utilised. More important and possibly more damaging than the former may be the implementation of an inadequate data and information security environment. From the previous examples, it is clear that the scope of use and the data content involved can be highly sensitive areas, so the data protection law's risk-based approach raises serious expectations. In this context, particular attention should be paid to the secure storing and transmission of data, as accidental/unlawful access (i.e. in the event of a data breach [Articles 32, 33 GDPR]) could lead to the endangering of entire digital identities. The issue of access to databases should also be mentioned here because although the

[18] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)

[19] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)

[20] Proposal for a regulation of the european parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts

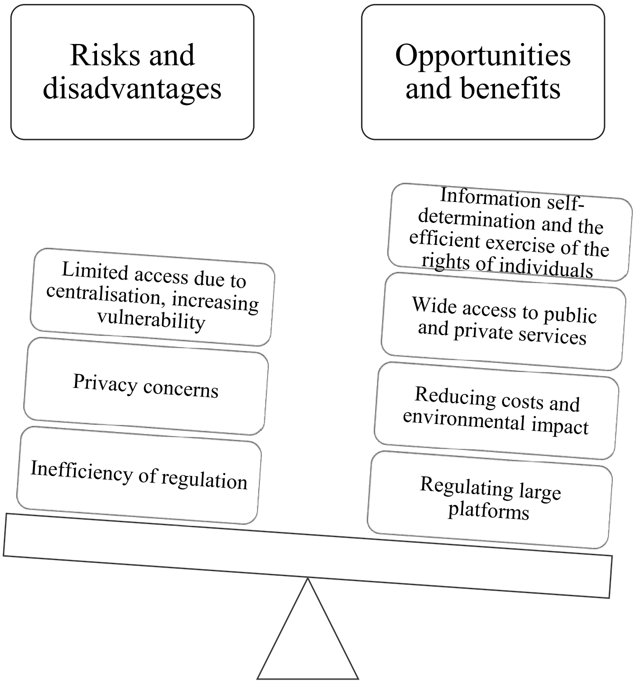
[21] Proposal for a regulation of the european parliament and of the council concerning the respect for private life and the protection of personal data in electronic communications and repealing directive 2002/58/ec (regulation on privacy and electronic communications)

[22] Member of the European Parliament (ECR)

proposal indicates that these databases can only be linked to the necessary extent, the legislator has raised an interpretative question which will certainly be answered differently in different Member States of the EU.

The provisions of the Regulation may prove ineffective. This may be due to user distrust or even widespread market resistance. In this case, most of the benefits will not be manifested, no reduction in the environmental impact and costs can be expected, and the Regulation will not contribute to a more efficient eGovernment and to reforming the position of large platforms.

Figure 1. Summary of possible impacts and consequences


Risks and disadvantages
Opportunities and benefits
Information self-determination and the efficient exercise of the rights of individuals
Limited access due to centralisation, increasing vulnerability
Wide access to public and private services
Privacy concerns
Reducing costs and environmental impact
Inefficiency of regulation
Regulating large platforms

Source: Authors' determination

## 5 National digital citizenship programme: digital citizenship – digital administration

### 5.1 From electronic to digital administration

The electronic handling of public administrations is just one of the "branching out" of the effects of technological developments on public administration. The need for change and change itself is evident, both from the state and from citizens and businesses. (Veale and Brass, 2019)

"In the past, customer needs were based on face-to-face interaction and paper-based administration, but with technological advances, mobile penetration and digital literacy have increased to such an extent that the need for a change of approach in this area has become clear. Customers now also expect public administrations to provide them with the autonomy to choose the path, solution or even the means to interact with the administration and address their problems." (Molnár, Sasvári and Tarpai, 2020).

In 2020 and 2021, changes to administrative legislation due to the pandemic, as well as individual management decisions have both pushed e-government to the forefront of administrative procedures, resulting in a significant drop in face-to-face contact with customers.[23]

The essence of electronic administration is contained in 8. (1) of the Eüsztv.: the electronic handling of (procedural) acts. " Unless provided otherwise by an Act or a government decree adopted by acting within original legislative power, a client may carry out administrative acts and make statements by electronic means before an electronic administration organ in the course administering his matters."

By *electronic procedure,* we mean an administrative procedure that is carried out in absentia, using all the elements of modern infocommunication means. However, the relevant legislation does not include this type of procedure in this sense but uses a different approach instead of this complex aspect. This is the concept of *electronic administration*[24]. Hence, the two concepts do not have the same meaning.

Finally, I must emphasise the complexity of electronic administration, which also poses considerable risks for the customer. Here, the complexity is not only technological but also legal.[25]

The first steps taken in Hungary from electronic to digital public administration are less legal and more of a "decisional" nature: "A new era in government IT has begun with the establishment of the Digital Hungary Agency (DMÜ). The DMÜ will be in charge of state duties related to e-government, IT, the unification of e-government and IT developments, electronic communications for government purposes, and ensuring the infrastructural feasibility of public administration IT (DMÜ Introduction, 2022).

In December 2022, the DMÜ issued the National Digital Citizenship Programme (hereinafter: the Program) (Program, 2022), which essentially sets out the technology-based development of the Hungarian public administration until the end of the first "strategic period" in 2026.

The Programme is a fundamental document, it contains provisions on the exploitation of the national data assets and the use of cloud technology, but its

[23] Horváth, T. Presentation on Issues that can be dealt with at the Government Office during a pandemic; Vas, R., Presentation on building authority procedures during the pandemic Administrative Procedural Law Online Professional Conference on Authority procedures in the pandemic period, (2021).

[24] About the background: Fábián, A., (2006). Gondolatok a Ket. elektronikus ügyintézésre vonatkozó szabályairól. Infokommunikáció és Jog. 2006/1.

[25] Presentations of Horváth and Vas (see footnote 61.)

most important point is the introduction of digital citizenship ("Jön a digitális magyar állampolgárság", 2022).

Achieving "digital citizenship" requires the development of a "coherent online system providing an excellent user experience, radically simplifying communication between citizens and different government departments (e.g. administration, information) and contributing equally to citizen satisfaction and to the optimisation of public administration" (The Programme covers several topics, but the most relevant is the Concept of Digital Citizenship.)

The Programme is explicitly designed to achieve the objectives of the digital identity initiative launched by the European Union, focusing on the creation of basic services and customer-friendly channels on a single platform, and on redefining the digital relationship between the state and citizens. In today's modern and digital environment, it is essential for citizens to be able to communicate and manage all their interactions with the State and its institutions in a convenient, simple and immediate way. For this purpose, aligned with the eIDAS 2.0 requirements, the Programme will place particular emphasis on the promotion and full availability For this purpose, aligned with the eIDAS 2.0 requirements, the Programme will place particular emphasis on the promotion and full availability of e-ID, ePost, eDocument Management and ePayment services for Hungarian users (Program, 2022 pp. 5-6.).

The term digital administration appears a total of 10 times in the 84-page document.[26] Although the Programme does not expressly define the concept of digital administration and its distinction from electronic administration, the main elements of its meaning can still be deduced relatively precisely.

The Programme approaches digital administration explicitly as a technological and not a legal advance. It does not even qualify digital administration as an objective of administrative reform, but it also considers the creation of the necessary legal conditions.

In the context of the Programme, digital administration[27] is primarily

a) a mobile phone application,
b) that would provide a "user experience",
c) and it is widely accessible for a large number of cases involving a high number of customers,[28]
d) essentially simple electronic means of administration leading to changes in the basic public registers: typically document administration, motor vehicle administration, registrations of civil status, educational administrative matters, pension administration and entries in the land register (Program, 2022, pp. 21).

[26] See pps. 9, 13, 21, 23, 26, 27, 67 és 75.

[27] The Program also uses the concept of „mobile administration": p23.

[28] „The transformation, starting in 2023, will be continuous, prioritising issues affecting a wider range of citizens (e.g.: renewal of ID cards, driving licences, car purchase, property purchase)." pp. 13.

One can agree with the statement that digital platforms in public administration and their use in the enforcement of public law is one of the future essences and realisations of the service principle and that the same principle can unfold when the state creates and operates digital platforms, (Giest and Samuels, 2023) but also when the customer chooses from the digital interfaces which one is most convenient for them and uses it in the course of their administration (Poysti, 2018). It is clear that the digital platform favoured by customers today is mobile technology.

## 5.2 Digital administration and existing legislation

The term "digital administration" does not exist in our current legislation. Act CL of 2016 on the General Administrative Procedure (hereinafter: the General Administrative Procedure Act) refers in several provisions to procedural legal facilities based on electronic, infocommunication technologies, their applicability and suitability, thereby essentially giving free passage even to "digital administration" as defined in the Programme.

The starting point is one of the fundamental principles of the General Administrative Procedure Act: *the principle of efficiency*. According to this principle: " In the interest of efficiency, the authority shall organise its activity in such a manner as to result in the least possible expense for all participants in the procedure and, without prejudice to the requirements of clarifying the facts of the case, for the procedure to be closed as expeditiously as possible with the application of advanced technologies." [General Administrative Procedure Act 4.]

On the basis of this provision, it can be argued that the "use of advanced technologies" will speed up the "conclusion" of the proceedings, in other words, ultimately the decision on the merits.[29] In fact, advanced technology can mean anything, but primarily the use of information and communication technologies: "the public authority must give priority to the use of advanced technologies in its proceedings and, of course, must organise its own work as efficiently as possible, with emphasis on the use of electronic administration." [Explanatory Memorandum of General Administrative Procedure Act 2-6.].

Efficiency in the administrative procedure (Kilényi, 1970) can therefore be understood in several dimensions: in terms of the client, the authority, and the procedure, but also in terms of the performance of administrative tasks in general, which in a given sector can be measured in forints. For example, in tax administration, the introduction of online cash registers, online invoicing systems or the Electronic Roadside VAT Control System could significantly increase the VAT revenues of the central budget (Varga, 2021).

The General Administrative Procedure Act regulates the "electronic procedure", or more precisely electronic administration, from the viewpoint of *communica-*

[29] The reasons for changes in foreign legislation are similar, see also: Marcos, A., C., (2016). Electronic Government Innovations in the New Spanish Administrative Framework. Legislation Revista Juridica de Castilla y Leon, 40.; Gedid, J., (2012). Administrative Procedure for the Twenty-First Century: An Introduction to the 2010 Model State Administrative Procedure Act. St. Mary's Law Journal, (44).

*tion*. This essentially means that the electronic way of contacting is a suitable tool to "steer" the customer's participation and communication with the authority towards an electronic platform instead of a "platform" of presence.

The relevant provision of the General Administrative Procedure Act is the "general rules for contacts". According to this provision, the authority may communicate with the client and the participants in the procedure by electronic means, both in writing and orally. The written electronic communication consists of electronic means defined in the Eüsztv.

A crucial point is the definition of *communication*. Communication essentially means communication between a client and a public authority, which may or may not include communication intended to have legal effect. On the other hand, the Regulation does not speak of electronic administrative procedures, but of electronic administration. In this respect, the concept of administration is not clear, but it is likely to include – in theory – all the elements of the administrative procedure that are recognised and regulated by the Eüsztv.

"It is a step forward that the legislator no longer strives only to make documents available electronically and to create interoperability between paper and electronic documents, but also refers to the electronic nature of certain aspects of the process." (Veszprémi, 2021).

In addition, the General Administrative Procedure Act stipulates – as a guarantee – that unless otherwise provided by law, the form of communication is to be chosen by the customer on the basis of information provided by the public authority. The customer may switch from the chosen means of contact to another means available to the public authority. In the event of a situation threatening life or serious harm, the authority shall choose the means of contact. [General Administrative Procedure Act 26.]

In addition to the traditional written form, the General Administrative Procedure Act also considers the electronic form defined by Eüsztv. as written form. Where electronic means are used, Eüsztv. states that a declaration may be deemed to be in writing if the declarant is identified electronically in accordance with certain rules and it is ensured that the electronic document served is the same as the document approved by the declarant [Eüsztv. 17. (2)]. Electronic communication that does not meet the requirements of the Eüsztv. (e.g. a simple e-mail exchange or a telephone call without identification) is considered as oral communication under the General Administrative Procedure Act.

Although the concept of digital administration is not explicitly clarified in the Programme, it can be concluded that digital administration is not the same as automatic administration. In a somewhat simplistic way, an automatic procedure is an electronic procedure (electronic administration) in which "human intervention", whether the client (electronic) or administrator interaction, is excluded *ex lege*.

It can also be stated that automatic decision-making may be used – subject to other conditions – in administrative proceedings initiated by public authorities on request and ex officio. This form of administration essentially limits or excludes the exercise of most clients' rights, in fact, only the right to legal remedy can be exercised.

A key part of the extension of automatic decision making could be the issuing of certificates and extracts from administrative records. This would not only increase the service capacity of public administrations, meaning a positive change for customers but could also reduce the workload of administrators (Kárpáti, 2020).

## 6 Conclusions

It can be concluded that the domestic (public administration) digital framework has an existing, usable and actually used digital service palette. These follow the guidelines set by eIDAS and aim to work in accordance with its requirements.

However, it can be seen that (as with other EU trends) the system is highly fragmented, with elements not or not sufficiently supporting each other, and a significant disconnect between the public and private sectors. There is also concern that the existing platforms are less customer-friendly than expected. The current digitalisation coverage of the Hungarian public administration is only 16% of the general administration out of all online transactions (Program, 2022).

The concepts of EU identity, identification and digital citizenship in the EU can easily be brought together, but this interoperability also has its prerequisites. Among these, the technological requirements seem to be the easiest to meet, while the legal preconditions are predicted to be more complex and problematic. We only have to refer back to the advantages and disadvantages detailed in the eIDAS 2.0 provisions. A number of conditions are already in place that make these objectives technically achievable, but creating the right legal environment and promoting the fulfilment of the conditions for this may be a major challenge. Even in the most optimal situation, the feasibility of enforcing and monitoring implementation and enforcement may be questionable, as without them legal policy objectives become unattainable and constituted rights and obligations become void.

In order for electronic administration to be an electronic public administration procedure, it is necessary to develop a procedural/administrative model for an administrative procedure implemented. This is currently absent.[30] The model (modelled process) of electronic public administration can be adapted to the framework of digital public administration, which could be the basis for a comprehensive national legislation adapting the eIDAS rules. The situation as visioned by the regulation is undoubtedly desirable, but without the necessary – social and technological – conditions for its implementation in the pub-

[30] For details of possible alternatives see also: Torma, A., (2008). Az ügyintézés és a közigazgatási munkafolyamatok modellezéséről. Miskolc University Press.

lic administration system and its effective application, it is difficult to imagine that it can meet the legislator's expectations in real life situations.

Legislation must meet the requirements to allow the customer to participate effectively in the electronic (digital) process (administration), replacing paper-based customer actions by post or in person, but ensuring the customer's rights under national and EU law (Kárpáti, 2020). The regulation of this model could lead to a general electronic procedural code that would or could replace the General Administrative Procedure Act in such procedures.

The third prerequisite is trust. Online platforms for both the digital society and digital public administrations. The reliability of platforms and trust in general is a precondition for appropriate, transparent and "clean" legislation (Poysti, 2018). This is where the legal and non-legal requirements of digital public administration converge.

The current Hungarian legal administrative regime is ready to meet the eIDAS 2.0 expectations, and it is apparent that a number of legal and technological solutions have been introduced in recent years that meet the preconditions for meeting the requirements, at a level that is acceptable in EU terms. However, to move to the next phase, the national administration will need to align its own law with this new management structure, in addition to the legal and infrastructural requirements of the Regulation. It would be important that the two systems do not coexist in parallel, but instead of hindering each other, they could both support Hungarian users on their way to a higher level of digitisation. In order to achieve this, it would appear to be a good approach to take into consideration the administrative, European Union and data protection law aspects discussed in this study and to implement them in a context-appropriate manner.

## References

Baranyi, B., Homoki, P., Kovács. T. (2018). Magyarázat az elektronikus ügyintézésről. Budapest Wolters Kluwer.

Commission Staff. (2014). Working Document Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) n° 910/2014 as regards establishing a framework for a European Digital Identity. At <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52021SC0124>, accessed 9 November 2023.

Council of the EU (2022). European digital identity (eID): Council makes headway towards EU digital wallet, a paradigm shift for digital identity in Europe. At <https://www.consilium.europa.eu/hu/press/press-releases/2022/12/06/european-digital-identity-eid-council-adopts-its-position-on-a-new-regulation-for-a-digital-wallet-at-eu-level/>, accessed 23 May 2023.

De Hert, P., (2008). Identity management of e-ID, privacy and security in Europe. A human rights view. Information Security Technical Report 13.

Determann, L., (2021). Electronic form over substance: Esignature laws need upgrades. Hastings Law Journal, 72(1385).

Digitális Jólét Nonprofit Kft. (2020). Magyarország Mesterséges Intelligencia Stratégiája 2020-2030.

Digitális Magyarország Ügynökség, (2022). Bemutatkozás. At <https://www.dmu.gov.hu/cikkek/bemutatkozas-dmu>, accessed 19 May 2023.

Digitális Magyarország Ügynökség. (2022). Nemzeti Digitális Állampolgárság Program.

EUR-LEX (17.03.2016). More secure transactions on the Internet. At <https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX%3A32014R0910>, accessed 19 May 2023.

EUR-LEX, More secure transactions on the Internet. (17.03.2016). At <https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX%3A32014R0910>, accessed 19 May 2023.

European Comission, (2020). Digital Identity for all European. At <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_hu>, accessed 19 May 2023.

European Comission, (2020). Strategy on Shaping Europe's Digital Future.

European Parliamentary Research Service. (2022). EPRS Policy Podcast – Updating the European digital identity framework.

Fábián, A. (2006). Gondolatok a Ket. elektronikus ügyintézésre vonatkozó szabályairól Infokommunikáció és Jog. 2006/1.

Gedid, J. (2012). Administrative Procedure for the Twenty-First Century: An Introduction to the 2010 Model State Administrative Procedure Act. St. Mary's Law Journal, (44).

Giest, S. and Samuels, A. (2023). Administrative burden in digital public service delivery: The social infrastructure of library programs for e-inclusion. Review of Policy Research, 40, pp. 626–645. https://doi.org/10.1111/ropr.12516.

Horváth, T. (2021). Presentation on Issues that can be dealt with at the Government Office during a pandemic. Vas, R., Presentation on building authority procedures during the pandemic Administrative Procedural Law Online Professional Conference on Authority procedures in the pandemic period.

hvg.hu (2022), Jön a digitális magyar állampolgárság: az ígéret úgy szól, hogy egy mobilos alkalmazással is azonosíthatjuk magunkat.

Kárpáti, O. (2020). Az elektronikus anyakönyvezés helye és szerepe a magyar közigazgatásban [Doctoral dissertation, ME ÁJK Deák Ferenc Állam- és Jogtudományi Doktori Iskola].

Kilényi, G., (1970). Az államigazgatási eljárás alapelvei. Budapest: KJK.

Marcos, A., C. (2016). Electronic Government Innovations in the New Spanish Administrative Framework. Legislation Revista Juridica de Castilla y Leon, 40.

McKinsey and Company. (2020). How COVID-19 has pushed companies over the technology tipping point—and transformed business forever. At <https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever#>, accessed 19 May 2023.

Molnár, L., Sasvári, P. and Tarpai Z., T. (2020). Közigazgatási informatikai alkalmazások. Budapest: Nemzeti Közszolgálati Egyetem.

NISZ Zrt. (2022). Ügyfélkapu elektronikus azonosítási szolgáltatás, ÁSZF v2.6.

NISZ Zrt. (2023). Központi azonosítási ügynök, ÁSZF v3.3

Poysti, T. (2018). Trust on Digital Administration and Platforms. Scandinavian Studies in Law 65.

Schwalm, S.and Alamillo-Domingo, I. (2022). Self-Sovereign-Identity & eIDAS: a Contradiction? Challenges and Chances of eIDAS 2.0*. European Review of Digital Administration and Law – Erdal 2021, 2(2).

Schwalm, S. (2023). The possible impacts of the eIDAS 2.0 digital identity approach in Germany and Europe. Conference paper, OpenIdentitySummit.

Schwalm, S. and Alamillo-Domingo, I. (2021). Self-Sovereign-Identity & eIDAS: a Contradiction? Challenges and Chances of eIDAS 2.0. European Review of Digital Administration & Law – Erdal, 2(2).

Solove, D., J. (2013). Privacy Self-Management and the Consent Dilemma", 126 Harvard Law Review.

Sullivan, C. (2016). Digital citizenship and the right to digital identity under international law. Computer law and security review, 32.

Szabó, M. D. (2012). Az információs hatalom alkotmányos korlátai, Miskolci Egyetem.

Torma, A. (2008). Az ügyintézés és a közigazgatási munkafolyamatok modellezéséről. Miskolc University Press.

Ubisecure-podcast (2022). eIDAS 2.0 and EU Digital Identity Wallet. At <https://www.youtube.com/watch?v=AQMmVxwxpEQ&t=20s>, accessed 13 September 2023.

Varga, Z. (2021). Digitalisierung in der ungarischen Steuerverwaltung. Miskolci Jogi Szemle, 1.

Veale, M. and Brass, I. (2019). Administration by Algorithm?: Public Management Meets Public Sector Machine LearningPublic Management Meets Public Sector Machine Learning. At <https://doi.org/10.1093/oso/9780198838494.003.0006.>, accessed on 19 May 2023.

Veszprémi, B. (2021). A stratégia-alkotástól a SZEÜSZ-ökig, elméleti alapok az e-közigazgatásban. Miskolci Jogi Szemle, 2021/1.

Weigl, L. et al. (2022). The EU's Digital Identity Policy: Tracing Policy Punctuations 15. International Conference on the Theory and Practice of Electronic Governance.