June 2024

Law Alert

Platis - Anastassiadis & Associates

The associate law firm of EY Greece

Regulation (EU) 2024/1183 – The New Framework for a European Digital Identity

On 11 April 2024, after a prolonged two-year negotiation process, the European Union has adopted Regulation (EU) 2024/1183 for the establishment of a European Digital Identity ("Regulation"). The Regulation is an act of general application, directly applicable in all Member States and does not require transposition into national law by law.

The new Regulation introduces extensive reforms of Regulation (EU) No 910/2014 ("e-IDAS Regulation"), the most important of which is the establishment of an effective EU-wide framework for European Digital Identity Wallet ("EDIW") schemes.

The main aim of the Regulation is to guarantee access to secure and reliable electronic identification schemes and services for all EU residents, fostering trust in online transactions with both public and private service providers, in line with the targets set out in the 2030 Digital Decade policy programme.

To this end, the Regulation lays down the conditions for the issuing of European Digital Identity Wallets by Member States. The Regulation also expands the list of trust services (as defined in its article 3 point 16) introducing new qualified trust services, namely electronic archiving services (Article 45g), electronic ledgers (Article 45h), the management of remote electronic signature (Article 29a) and seal creation devices (Article 39a).

In parallel, the Regulation upholds fundamental rights, by upgrading the protection of personal data and empowering EU residents to securely request, select, combine, store, delete, share, and present data related to their identity, under their sole control, while enabling selective disclosure.

1. Reforming the e-IDAS Regulation

The evaluation of the e-IDAS Regulation by the European Commission has brought to light several shortcomings, outlining challenges and concerns that have surfaced since its implementation, such as: Difficulties in Connecting Online Private Providers:

- Difficulties in Connecting Online Private Providers: One notable limitation pertains to challenges in integrating online private providers into the e-IDAS system seamlessly, potentially hindering the broad participation of diverse service providers.
- Limited Cross-Border Access: Since the implementation of the e-IDAS Regulation, only 14 Member States have notified electronic Identity schemes (eIDs). This has resulted in a restricted cross-border access to services scenario for EU residents. The low number of participating Member States has implications for the interoperability and widespread availability of digital identity solutions across the EU.
- Privacy and Data Protection Concerns: The eIDs provided by social media entities and financial institutions have raised legitimate concerns regarding privacy and data protection. Therefore, there were shortcomings in the ability of these solutions to meet evolving market demands and the absence of robust cross-border capabilities, particularly in sectors dealing with sensitive information.
- Lack of Coverage for Electronic Attributes: The e-IDAS Regulation falls short in covering electronic attributes, such as medical certificates or professional qualifications. This deficiency poses a challenge to achieving pan-European legal recognition, as these electronic attributes play a crucial role in various sectors, including healthcare and professional accreditation.
- Given the need for reform of the e-IDAS Regulation, the new Regulation has been introduced in order to enhance connectivity with private providers, expand cross-border access, ensure widespread availability of eIDs, address privacy concerns, and broaden the coverage of electronic attributes for a more robust and inclusive digital identity framework in the EU.

2. Scope, Definitions & Subject Matter

The Regulation applies to electronic identification schemes that have been notified by a Member State, European Digital Identity Wallets issued by Member States and to trust service providers that are established in the Union.

According to the Regulation, the following definitions apply to trust services:

- European Digital Identity Wallet: A product and service that allows the user to store identity data, credentials and attributes linked to her/his identity, to provide them to relying parties on request and to use them for authentication, online and offline, for a service; and to create qualified electronic signatures and seals.
- Electronic attestation of attributes: An attestation in electronic form that allows the authentication of features, characteristics or qualities of a natural or legal person or of an entity.
- Electronic archiving: A service ensuring the receipt, storage, deletion and transmission of electronic data or documents in order to guarantee their integrity, the accuracy of their origin and legal features throughout the conservation period.
- Electronic ledger: A tamper proof electronic record of data, providing authenticity and integrity of the data it contains, accuracy of their date and time, and of their chronological ordering.

Furthermore, the Regulation introduces the following new trust services:

1) the creation, verification, and validation of electronic registered delivery services,
2) the electronic attestation of attributes and certificates related to those services;
3) the management of remote electronic signature creation devices and preservation services;
4) the creation, verification and validation of certificates for website authentication;
5) the electronic archiving of electronic documents;
6) the recording of electronic data into an electronic ledger.

Verification of the identity and, if applicable, any specific attributes of natural or legal persons shall be conducted by qualified trust service providers, either directly or by relying on a third party, either by means for physical presence or by means of a notified electronic identification means or by using other identification methods which ensure the identification of the natural person with a high level of confidence, the conformity of which shall be confirmed by a conformity assessment body.

Trust service providers are required under the Regulation to have in place appropriate policies and measures to manage legal, business, operational and other direct or indirect risks to the provision of the qualified trust service, including: (i) measures related to registration and on-boarding procedures to a service; (ii) measures related to procedural or administrative checks; (iii) measures related to the management and implementation of services.

Electronic attestations of attributes have the equivalent legal effect of lawfully issued attestations in paper form and, therefore, shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that they are in an electronic form or that they do not meet the requirements of the qualified electronic attestation of attributes.

Qualified certificates for website authentication shall be recognised by web-browsers. For those purposes web-browsers shall ensure that respective identity data are displayed in a user friendly manner. Web-browsers shall ensure support and interoperability with qualified certificates for website authentication.

Qualified electronic archiving services for electronic documents are provided by qualified trust service providers that use procedures and technologies capable of extending the trustworthiness of electronic documents beyond the technological validity period.

An electronic ledger combines time stamping of data and their sequencing with certainty about the data originator similar to e-signing with the additional benefit of enabling a more decentralized governance that is suitable for multi-party cooperation. An electronic ledger shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic ledgers. A qualified electronic ledger shall enjoy the presumption of the uniqueness and authenticity of the data it contains, of the accuracy of their date and time, and of their sequential chronological ordering within the ledger.

3. The Regulation of EDIWs

The ecosystem of EDIWs consists of the following stakeholders:

- Issuers: Member states or private entities mandated or appointed by member states.
- Certifying Bodies: Accredited public or private sector bodies designated by Member States certifying the conformity of EDIWs with the requirements of the Regulation in line with the European cybersecurity certification framework, as established by the Cybersecurity Act, and the certification schemes established by the GDPR.
- Relying Parties: Upon notification to competent national authorities, public sector bodies and private entities providing services in areas (e.g. basic services) where strong user authentication for online identification is required by national or Union law or by contractual obligation may become relying parties of EDIWs.
- Certifying Bodies: Accredited public or private sector bodies designated by Member States certifying the conformity of EDIWs with the requirements of the Regulation in line with the European cybersecurity certification framework, as established by the Cybersecurity Act, and the certification schemes established by the GDPR.
- Users: The end-users of EDIWs and trust services linked to them.

EDIWs ensure unique offline and online identification by incorporating unique and persistent identifiers of their users. They, thus, enable their users to (a) securely request and obtain, store, select, combine and share identification data and electronic attestation of attributes to authenticate online and offline in order to use online public and private services; and (b) sign by means of qualified electronic signatures. EDIWs act as means to execute these functions by providing a common interface for relying parties to request, receive and validate person identification data and electronic attestations of attributes, thus authenticating their users.

The use of EDIWs is free of charge to natural persons, while users are vested with their full and exclusive control. EDIWs are required to comply with the highest level of security for the personal data used for authentication irrespective of whether such data is stored locally or on cloud-based solutions, taking into account the different levels of risk.

Acceptance of EDIWs is compulsory for digital public services across the Union and, also, for digital private services, notably for VLOPs and where strong assurance of electronic identification is needed, as is the case for credit, payment and other financial services and for use cases related to the provision of basic services.

Prior to being put into use, EDIWs are required to be certified under a cybersecurity scheme pursuant to Regulation (EU) 2019/881 ("Cybersecurity Act") and a data protection certification scheme pursuant to Regulation (EU) 2016/679 ("GDPR").

Cross-border reliance of EDIWs is guaranteed by way of an explicit obligation in the Regulation for national public sector bodies of member states to accept EDIWs issued in accordance with its provisions.

Accordingly, where they require users to authenticate to access online services, very large online platforms as defined in Article 25.1. of the Digital Service Act are required to accept the use of European Digital Identity Wallets upon voluntary request of the user. Users shall be under no obligation to use the wallet to access private services, but if they wish to do so, large online platforms will be required to accept the European Digital Identity Wallet for this purpose while respecting the principle of data minimization.

4. Additional Safeguards

The Regulation incorporates a set of enhanced safeguards to ensure the integrity and privacy of users, which, among others, include the following:

- Measures against Data Misappropriation: Trust service providers are required to take appropriate measures against forgery, theft or misappropriation of data or, without right, deleting, altering or rendering data inaccessible.
- Right to Pseudonymity (Article 5): Recognizing the importance of online anonymity, the Regulation enforces the right to pseudonymity. Users can use locally stored pseudonyms, providing a layer of privacy. However, this right is subject to potential restrictions imposed by national and EU law.
- Selective Disclosure: The EDIWs technically enable the selective disclosure of attributes to relying parties as their basic design feature, thereby reinforcing convenience and personal data protection, including data minimisation (Recital 29).
- Privacy and Security: EDIWs are designed to empower users by providing a secure platform. Users have the right to seamlessly request, obtain, store, select, combine, and share necessary legal person identification data and electronic attestation of attributes. This process is conducted in a transparent and traceable manner, facilitating user authentication both online and offline (Article 6a).

According to the provisions of the Regulation, trust service providers shall be obliged to be audited at their own expense at least every 24 months by independent conformity assessment bodies regarding their compliance and the compliance of their qualified trust services with the requirements laid down in the amended e-IDAS Regulation and in Article 18 of the NIS2 Directive.

Trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation and with the cybersecurity risk management obligations under Article 18 of the NIS2 Directive.

5. Timeline

The Regulation enters into force on the 20th day following its publication in the Official Journal of the EU, i.e. on 30 May 2024.

Within 6 months of the entering into force of the Regulation, the Commission shall by means of implementing acts, among others, (i) establish technical and operational specifications and reference standards for the implementation of EDIWs; (ii) establish a list of standards for the certification of EDIWs; and (iii) establish a list standards for qualified electronic attestations of attributes.

Within 12 months of the entering into force of the Regulation, the Commission shall also by means of implementing acts (i) specify the tasks of national supervisory authorities of the amended e-IDAS Regulation, and (ii) specify conformity assessment schemes and auditing requirements.

Within 12 months after the entry into force of the Regulation, each Member State shall issue a European Digital Identity Wallet.

To ensure that Member States will be ready to provide EDIWs by the deadline set in the Regulation, the Commission is working with Member States on a Toolbox of technical aspects to build the prototype European Digital Identity Wallet app.

The Commission is also already investing €46 million from the Digital Europe Programme in four large-scale pilots, to test the EU Digital Identity Wallet in a range of everyday use-cases, including the Mobile Driving Licence, eHealth, payments, and education and professional qualifications.

6. Key Takeaways

Overall, the Regulation brings about the following deep reforms vis-à-vis the e-IDAS Regulation:

- Establishes the EDIW framework and lays down the institutional rules for the eID services universally accessible and acceptable across the Union.
- Enhances security and privacy safeguards to protect the fundamental rights of EU residents.
- Improves cross-border electronic identification between member state authorities.

Especially, EDIWs shall take the form of easy-to-use personal digital wallets, in the form of apps, allowing EU residents to digitally identify themselves in an immediate, safe and efficient manner, when using online public and private services, and, also, to store and manage identity data and official documents in digital form.

The Regulation (EU) 2024/1183 is available here.

About Platis – Anastassiadis & Associates

Platis - Anastassiadis & Associates is part of the EY Law network operating in 90 countries globally and is comprised of 3,500+ people.

We are an independent law office with a core team of 45 lawyers. Our office provides high quality legal services across the full range of commercial and financial transactions.

Especially in our geographical area, we have established an ongoing cooperation with the respective law firms which are associated with EY, in order to offer seamless and consistent regional services to our clients that have cross country operations.

Our experience allows us to better understand our clients' needs and offer them integrated multidisciplinary solutions in the fields of accounting, tax and financial advisory services. Platis – Anastassiadis & Associates law office is solution focused. We work closely with our clients to seek innovative and practical ways of dealing with their issues. Our priority is to help our clients meet their business objectives. Our expertise, commitment and enthusiasm has resulted in the build up of a client base which includes local and international listed, state and private sector companies and financial institutions.

For more information on digital law issues, please contact:

Eirinikos Platis
Partner
Tel.: +30 210 2886 521
eirinikos.platis@gr.ey.com

Antonios Broumas
Senior Manager
Tel.: +30 210 6171 502
antonios.broumas@gr.ey.com

at the
Platis - Anastassiadis & Associates Law Partnership
Tel.: +30 210 2886 512
platisanastassiadis@gr.ey.com

ey.com

EY EY Greece eygreece @EY_Greece EY Greece

Platis - Anastassiadis & Associates Law Partnership is associated with EY.
Partners: E. Platis, A. Anastassiadis
Partnership is registered with the Athens Bar, registration number 80240
List of our associates upon request.