DEBRIEFING

REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

Berlin, 02.07.2024

Law / Legal Act: REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

Publication Date: 30.04.2024
Entry into Force : 20.05.2024
Reference: REGULATION (EU) 2024/1183
Applies to: Trust services, providers of web-browser, providers of public and private services
Content: The Regulation amends the eIDAS Regulation of 2014 and establishes the basis for European Digital Identity Wallets. In addition, the Regulation contains new provisions for providers of web-browsers in connection with the recognition of qualified website authentication certificates (QWACs).

What does the law regulate?

The Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation/Regulation No. 910/2014) was first adopted in 2014 and has been in force since 2016. Its aim was to increase the use of trust services for cross-border transactions in the digital space through harmonised Europe-wide standards in the field of online signatures, electronic seals and digital identities. The amendment now extends the Regulation and includes, inter alia, a framework for European Digital Identity Wallets. In addition, providers of web-browsers will be required to recognise qualified website authentication certificates (QWACs).

I. European Digital Identity Wallets

The provisions listed under Section I refer to the European Digital Identity Wallets regulated under the Regulation. They apply to the providers of these wallets, the users and the providers of private and public services.

1. Provision and functions of the wallets, in accordance with Article 5a
    a. Member States are obliged under Article 5a (1) to provide at least one European Digital Identity Wallet for all natural and

legal persons in the Union by **November 2026**. According to paragraph 15, the use of such a wallet is voluntary.

b. In accordance with Article 5a (2), the wallet may be issued either directly by a Member State, under a mandate from a Member State, or independently of a Member State but recognised by that Member State.
c. The issuance, use and revocation of the European Digital Identity Wallets shall be free of charge to all natural persons, in accordance with Article 5a (13).
d. The source code of the application software components of the European Digital Identity Wallets must be subject to an open-source licence.
e. In accordance with Article 5a (4), the wallets provided shall enable the following functions:
    i. securely request, obtain, select, combine, store, delete, share and present electronic attestations of attributes and person identification data and, where applicable, in combination with electronic attestations of attributes, to authenticate relying parties online and offline, while ensuring that selective disclosure of data is possible;
    ii. generate pseudonyms and store them encrypted and locally within the wallets;
    iii. securely authenticate another person's wallet and receive and share – between the two wallets – person identification data and electronic attestations of attributes;
    iv. access a log of all transactions carried out through the wallet via a common dashboard;
    v. sign by means of qualified electronic signatures or seal by means of qualified electronic seals;
    vi. download, to the extent technically feasible, the user's data, electronic attestation of attributes and configurations.
f. In addition, the wallets must support common protocols and interfaces that enable the functions specified in Article 5a (5).
g. Member States may provide, in accordance with national law, additional functionalities of European Digital Identity Wallets, including interoperability with existing national electronic identification means.
h. The European Digital Identity Wallets shall also meet the requirements of Article 8 with regard to assurance level high.
i. In accordance with Article 5a (24), the Commission shall by **21 November 2024 establish** further specifications for the wallets by means of implementing acts.

2. Requirements for personal data protection
    a. In accordance with Article 5, without prejudice to specific rules of Union or national law requiring users to identify themselves, the use of pseudonyms shall not be prohibited.
    b. In accordance with Article 5a (b), wallets shall ensure that trust service providers of electronic attestations of attributes shall not provide any information about the use of those electronic attestations after they have been issued.
    c. In accordance with Article 5a (14), the provider of a European Digital Identity Wallet must not collect any information about the use of a wallet that is not necessary for the provision of the services, nor combine personal data from any other services offered by that provider or from third-party services, unless the user has expressly requested otherwise.
    d. Personal data relating to the provision of the European Digital Identity Wallets shall be kept logically separate from any other data held by the provider. If the wallet is provided by private parties, the provisions of Article 45h (3) shall apply *mutatis mutandis*.
3. Certification of the European Digital Identity Wallets
    a. In accordance with Article 5c (1), the conformity of the European Digital Identity Wallets with the requirements laid down in Article 5a (4), (5) and (8), with the requirement for logical separation laid down in Article 5a (14) and, where applicable, with the standards and technical specifications referred to in Article 5a(24), shall be certified by conformity assessment bodies designated by Member States.
    b. Certification in relation to cybersecurity requirements shall be carried out in accordance with Regulation (EU) 2019/881 (Cybersecurity Act).
    c. By **21 November 2024**, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the certification.
    d. In accordance with Article 5c (4), certification shall be valid for up to five years, provided that a vulnerability assessment is carried out every two years. Where a vulnerability is identified, the certification shall be cancelled.
    e. In accordance with Article 46e (1), Member States shall inform the Commission and the Cooperation Group established without undue delay of European Digital Identity Wallets that have been provided pursuant to Article 5a and certified by the conformity assessment bodies referred to in Article 5c (1).
4. Security breaches of the European Digital Identity Wallets
    a. In accordance with Article 5e (2), if the security breach or compromise is not remedied within three months of the

suspension, the Member State that provided the Digital Identity Wallets shall withdraw these wallets and revoke their validity.

b. By **21 November 2024**, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish the specifications and procedures for the measures referred to in Article 5e in the case of a security breach of Digital Identity Wallets.

5. Recognition
   a. Where Member States require electronic identification and authentication to access an online service provided by a public sector body, they shall also accept European Digital Identity Wallets that are provided in accordance with Article 5f (1) of the Regulation.
   b. Private relying parties that provide services in certain sectors are required under Article 5f (2) to accept European Digital Identity Wallets as a means of authentication if online identification with strong user authentication is contractually obliged. This applies, for example, to providers of private services in the areas of transport, energy, banking, financial services, social security, health, drinking water, postal services, digital infrastructures, education or telecommunications. In addition, acceptance is also mandatory for those private relying parties that are required by Union or national law to use strong user authentication for online identification. Exceptions are only provided for microenterprises or small enterprises. **This applies 36 months after the entry into force of the corresponding implementing acts. These are to be published by the Commission in accordance with Articles 5a (23) and 5c (6) by 21 November 2024.**
   c. In accordance with Article 33 of the Digital Services Act, very large online platforms (VLOPs) are required by Article 5f (3) to accept Digital Identity Wallets if user authentication is required for access to online services and the user requests this.

II. Provisions for providers of web-browsers in accordance with Article 45

The provisions listed under Section II apply in particular to providers of web-browsers and issuers of qualified website authentication certificates (QWACs).

1. Obligation of recognition of QWACs
   a. According to Article 45 (1a), qualified certificates for website authentication issued in accordance with paragraph 1 of the

Article shall be recognised by providers of web-browsers. In addition, providers of web-browsers are required to ensure that the identity data attested in the certificate and additional attested attributes are displayed in a user-friendly manner.

b. In accordance with Article 45 (1), QWACs must comply with the requirements laid down in Annex V.
c. In accordance with Article 45 (2), by **21 May 2025**, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified certificates for website authentication, as referred to in Article 45 (1).
d. In accordance with Article 45a (2), the obligations laid down in Article 45 may only be deviated from in cases of substantial concerns related to security breaches or the loss of integrity of an identified certificate or set of certificates.

III. Application and enforcement

The provisions listed under Section III concern the application, enforcement and governance of the amended eIDAS Regulation.

1. Application
   a. The provisions of the Regulation are applicable upon entry into force 20 days after publication in the Official Journal of the EU. **The obligation to provide European Digital Identity Wallets free of charge for all citizens will apply from 2026.**
   b. Transitional measures are set out in Article 51.
   c. By 21 May 2030 and every four years thereafter, the Commission shall submit a report to the European Parliament and the Council on progress made towards achieving the objectives of this Regulation.
2. Enforcement
   a. In accordance with Article 16 (1), Member States shall lay down the rules on penalties applicable to infringements of this Regulation. Those penalties shall be effective, proportionate and dissuasive.
   b. Member States shall ensure that infringements of this Regulation by qualified and non-qualified trust service providers are subject to administrative fines with a maximum level of at least 5 million Euro for trust service providers that are natural persons or 5 million Euro or 1 % of the total worldwide annual turnover for trust service providers that are legal persons.
3. Governance
   a. Member States shall designate one or more supervisory bodies to supervise Digital Identity Wallets in accordance with Article 46a.

b. In accordance with Article 46c, Member States shall also designate single point of contacts for trust service providers, providers of Digital Identity Wallets and notified electronic identification schemes. This shall exercise a liaison function to facilitate cross-border cooperation between the supervisory bodies.
c. In Germany, the German Federal Network Agency (BNetzA) was designated as the supervisory authority for the eIDAS Regulation by the German Trust Services Act (VDG). The German Federal Office for Information Security (BSI) is the competent supervisory authority for providers of website certificates.
d. Article 46e also introduces a European Digital Identity Cooperation Group. This shall be composed of representatives appointed by the Member States and the Commission and shall serve to promote cross-border cooperation and exchange of information.

About eco: With approximately 1,000 member companies, eco (international.eco.de) is the leading Association of the Internet Industry in Europe. Since 1995, eco has been highly instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of its members in politics and international forums. eco has offices based in Cologne, Berlin and Brussels. In its work, eco primarily advocates for a high-performance, reliable and trustworthy ecosystem of digital infrastructures and services.