

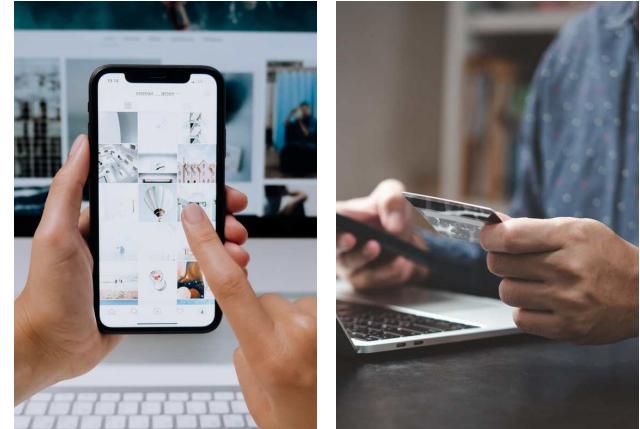
DIGITAL IDENTITY WALLET RECHTSKONFORM UMSETZEN



■ eIDAS-2-Konformität | Verlässlich integriert.
Digitale Identität | Sicher bereitgestellt.
Vertrauensdienste | Nutzerzentriert gestaltet.

Überblick

Die eIDAS-2.0-Verordnung regelt die Anforderungen an die sichere Bereitstellung und Nutzung digitaler Identitäten in der EU von Behörden bis zu privaten Dienstleistern. Digitale Identitätsnachweise eröffnen bereits heute in Verwaltung, Wirtschaft und Alltag neue Wege für Vertrauen und Effizienz, etwa durch standardisierte Wallets, interoperable Schnittstellen oder datenschutzkonforme Authentifizierung. Mit eIDAS 2.0 schafft die EU einen einheitlichen Rechtsrahmen. Doch die Einführung der EUDI-Wallet bringt auch technische und organisatorische Herausforderungen mit sich, denn Organisationen müssen Identitätsdaten sicher verarbeiten, Zugriffsrechte korrekt steuern und die Nutzbarkeit über nationale Grenzen hinweg gewährleisten.



Betroffene Unternehmen (Auszug)

Verpflichtete Organisationen

Organisationen, die digitale Identitätsdienste bereitstellen oder **nutzen** (z. B. Behörden, Banken, Plattformanbieter, Mobilitätsdienste), müssen sicherstellen, dass ihre Systeme die Anforderungen der eIDAS-2.0-Verordnung erfüllen und mit der EUDI-Wallet interoperabel sind.

Vertrauensdienste und Schnittstellenanbieter

Unternehmen, die Identitätsdaten verarbeiten oder Wallet-Funktionen integrieren, müssen gewährleisten, dass ihre Dienste den Vorgaben zu Sicherheit, Interoperabilität und Datenschutz genügen. Dazu gehören technische Standards, Schnittstellenprotokolle und Zertifizierungsanforderungen.

Unternehmensgröße

Die eIDAS-2.0-Verordnung gilt unabhängig von der Unternehmensgröße für alle Anbieter und Nutzer digitaler Identitätsdienste.

Geografische Reichweite

Die Verordnung betrifft alle Organisationen, die digitale Identitätsdienste in der EU bereitstellen oder nutzen auch mit Sitz außerhalb der EU.

Ausnahmen

Es gibt keine Ausnahmen, die Regelungen der Verordnung gelten für alle Unternehmen, welche die Nutzung digitaler Identitätsdienste anbieten oder anbieten müssen

Sanktionen

Bei Verstößen gegen die eIDAS 2.0-Verordnung sind die Mitgliedstaaten verpflichtet, Sanktionen festzulegen, die wirksam, verhältnismäßig und abschreckend sind. Je nach Art und Schwere des Verstoßes können dabei empfindliche Geldbußen verhängt werden. Diese können sich auf bis zu 5 Millionen Euro belaufen oder bei juristischen Personen bis zu 1 % des weltweiten Jahresumsatzes betragen. Mögliche Verstöße sind beispielsweise die unsachgemäße Verarbeitung von Identitätsdaten, fehlende Interoperabilität, eine unzureichende Sicherheitsarchitektur oder falsche bzw. irreführende Angaben zur Funktionsweise der Wallet oder zu Vertrauensdiensten.

Fristen

20. Mai 2024: Die eIDAS-2.0-Verordnung ist in Kraft getreten.

Seit **November 2024**: Die EU-Kommission erlässt Durchführungsrechtsakte mit den technischen Spezifikationen für die EUDI Wallets (40 sind insgesamt vorgesehen).

Bis Anfang 2027 (voraussichtlich): Die Mitgliedstaaten müssen die EUDI Wallets, die den neuen Anforderungen an Sicherheit und Interoperabilität entsprechen, für ihre Bürger bereitstellen. Die meisten Experten gehen von einer Verfügbarkeit im Laufe des Jahres 2026 aus.



Neue Pflichten (Auszug)

Anbieter digitaler Identitätsdienste

- Wallet-Systeme müssen interoperabel, sicher und datenschutzkonform bereitgestellt werden
- Geeignete technische und organisatorische Maßnahmen zur Attributverifizierung umsetzen
- Verfügbarkeit und Integrität der Wallet-Funktionen auch bei Störungen sicherstellen
- Sicherheitsrelevante Informationen vollständig und fristgerecht dokumentieren
- Zusätzliche Prüfpflichten für eingesetzte Komponenten und Schnittstellen beachten
- Meldepflichten bei Sicherheitsvorfällen gem. eIDAS-Vorgaben einhalten

Nutzer der EU Digital Identity Wallet

- Wallets müssen zuverlässig nutzbar und gegen Manipulation geschützt sein
- Digitale Identitätsdaten sind sicher zu verwalten und kontrolliert weiterzugeben
- Geeignete Verfahren zur Wiederherstellung und Zugriffssicherung sind vorzusehen
- Physische und digitale Schutzmaßnahmen für Endgeräte und Anwendungen beachten
- Vertrauenswürdige Dienste müssen transparent und nachvollziehbar nutzbar sein
- Sensibilisierung zur sicheren Nutzung und Verwaltung der Wallet regelmäßig fördern

Unsere Beratung zur EUDI Wallet

Initialanalyse und Bestandsaufnahme

- Prüfung, ob und wie Organisationen von der eIDAS-2.0-Verordnung betroffen sind (EUDI-Betroffenheitsanalyse)
- Identifikation von Pflichten, Integrationsanforderungen und Anpassungsbedarf
- GAP-Analyse

Wallet-Integration und Vertragsprüfung

- Unterstützung bei der Einführung von Wallet-kompatiblen Identitätsdiensten
- Beratung zur vertraglichen Absicherung technischer und organisatorischer Anforderungen

Governance und technische Umsetzung

- Entwicklung interner Prozesse zur Attributverifizierung und Zugriffskontrolle
- Begleitung bei der Einführung von Sicherheitsmaßnahmen und Schnittstellenstandards

Dokumentation und Transparenz

- Erstellung technischer Unterlagen und Nachweise zur Wallet-Konformität
- Bereitstellung relevanter Informationen für Behörden und Vertrauensdienste
- Schulung von Geschäftsleitung und Mitarbeitern

Streitbeilegung und Behördenkommunikation

- Unterstützung bei der Einrichtung von Melde- und Kommunikationsprozessen
- Begleitung bei Anfragen öffentlicher Stellen und regulatorischen Verfahren

Kostenstruktur und Fairnesskontrolle

- Prüfung von Gebührenmodellen für Wallet-Dienste auf Angemessenheit
- Beratung zur Einhaltung gesetzlicher Vorgaben bei Nutzerkommunikation und Dienstgestaltung

Vertrauen Sie auf unsere Expertise –
als starker Partner für rechtssichere
und praxisnahe Lösungen rund um das
Thema EUDI Wallet.



Dr. Hans Markus Wulf
Rechtsanwalt | Partner
Fachanwalt für IT-Recht
ISO/IEC 27001 Auditor (TÜV)
CIPP/E, Datenschutzauditor (TÜV)

m.wulf@heuking.de

Berlin
Chemnitz
Düsseldorf
Frankfurt

Hamburg
Köln
München
Stuttgart



heuking.de