

16 JULY 2025

# A practical vision for the European Business Wallet

## Executive summary

DIGITALEUROPE welcomes the European Commission's initiative to develop a European business wallet (EBW), as announced in the 2025 Commission Work Programme and to build upon the EU Digital Identity Framework.<sup>1</sup> The EBW is intended to address long-standing fragmentation in the way businesses identify themselves, share credentials, and interact with public administrations and other economic operators across the EU.

Today, reporting obligations and regulatory procedures for companies are handled through a mix of paper-based processes, disconnected portals and non-standardised formats. This creates duplication, legal uncertainty and unnecessary administrative overhead – particularly for SMEs and cross-border operators. Inconsistent national rules and technical infrastructures further exacerbate the problem, restricting access to services and slowing the uptake of digital solutions.

The EBW aims to respond to these challenges by introducing a secure, interoperable and EU-wide identity solution for legal persons. It will enable economic operators to identify and authenticate themselves, receive official notifications and share verifiable credentials across borders – including permits, licences, certificates or VAT registration. The EBW is expected to support interactions across business-to-government (B2G), business-to-business (B2B) and government-to-government (G2G) contexts.

To fully realise these objectives, DIGITALEUROPE encourages an in-depth discussion on making the Business Wallet mandatory for the public sector and for specific use cases. Voluntary uptake alone will not deliver the legal certainty, harmonisation or efficiency gains that the initiative sets out to achieve. A regulated, obligation-based model – grounded in interoperability with the EU Digital Identity Wallet and existing trust services – is essential to ensure consistent implementation across Member States and promote uptake amongst businesses of all sizes.


To support the development of a practical and future-ready solution, this paper puts forward recommendations that call for:

- ▶▶ Prioritising high-value, B2B and cross-border use cases beyond administrative simplification;
- ▶▶ Introducing harmonised identity structures and mandate management;

---

<sup>1</sup> Regulation (EU) 2024/1183.



- 
- ▶▶ Ensuring flexibility in implementation and openness to private-sector innovation;
  - ▶▶ Embedding security, fraud resilience and accountability from the outset;
  - ▶▶ Designing for international interoperability and scalable data standards;
  - ▶▶ Making the business wallet mandatory for the public sector and for specific use cases; and
  - ▶▶ Covering all types of legal organisational forms, economically active individuals, including self-employed individuals.



## Table of contents

|  |          |
|--|----------|
| <b>Executive summary .....</b>   | <b>1</b> |
| <b>Table of contents .....</b>   | <b>3</b> |
| <b>Key challenges.....</b>   | <b>4</b> |
| <b>Key recommendations .....</b>   | <b>4</b> |
| <b>1. Start with real business needs, not just administrative simplification .....</b> | <b>4</b> |
| <b>2. Embed trust through harmonised identity and mandate structures .....</b>         | <b>5</b> |
| <b>3. Ensure flexibility in implementation and openness to innovation .....</b>        | <b>5</b> |
| <b>4. Embed strong security and accountability mechanisms .....</b>                    | <b>5</b> |
| <b>5. Enable international interoperability and scalable data standards .....</b>      | <b>6</b> |



## Key challenges

Despite progress in digitalising identity systems for natural persons, the EU still lacks a unified legal and technical infrastructure to support business identity, representation and regulatory compliance. Economic operators – including SMEs and self-employed professionals – continue to face complex and fragmented procedures when interacting with public authorities or private-sector partners across borders.

Today, most reporting and administrative obligations are fulfilled through country-specific systems, physical documentation or separate digital platforms that are not interoperable. These processes are time-consuming, inconsistent and disproportionately burdensome for smaller firms. Many Member States maintain their own document formats, identity verification channels and registry structures, resulting in limited mutual recognition and duplicated efforts.

In addition, there is currently no standardised EU-wide mechanism for representing company mandates and delegated authority. This means that verifying who is legally authorised to act on behalf of a company remains a national exercise, often reliant on manual checks, power-of-attorney paperwork or unverified declarations. As a result, cross-border contractual or licensing procedures often require significant additional effort, creating delays and compliance risks.

The absence of a harmonised approach limits the digital single market's effectiveness. It discourages automation, inhibits trust in cross-border exchanges and slows down transactions in both B2G and B2B settings. This problem affects not only regulatory reporting, but also supplier onboarding, due diligence and licensing processes – areas where efficient, trusted and legally recognised digital interaction is increasingly essential.

The EBW has the potential to address these issues by introducing a legally recognised, interoperable identity solution tailored to economic operators. However, to be effective, it must resolve these fragmentation issues at both the legal and technical levels – and be rolled out in a way that ensures universal adoption and legal clarity across Member States.

## Key recommendations

Against this backdrop, DIGITALEUROPE proposes the following principles to guide the development of a future-proof European Business Wallet.

### Start with real business needs, not just administrative simplification

The EBW should be developed around high impact use cases that reflect the operational needs of businesses and bring in most added value. These include the ability to digitally prove a legal person's identity, share verified credentials, attestations, mandates and fulfil legal obligations in cross-border contexts. Priority should be given to functions such as onboarding, licensing, ESG disclosures and public procurement – all of which require trusted identity and data exchange. Focusing only on B2G reporting would limit the wallet's added value and adoption. The EBW should also be clearly differentiated from the tools available under the Single Digital Gateway Regulation.<sup>2</sup>

---

<sup>2</sup> Regulation (EU) 2018/1724.

## Embed trust through harmonised identity matching and mandate structures

To ensure legal certainty the EBW should rely on EU-wide cross-border identity matching for all legal entities and economically active individuals (including self-employed individuals), leveraging existing registries and solutions to provide flexibility and avoid duplication. This should be supported by a standardised approach to role and mandate management, allowing the designation of authorised representatives and linking them to clearly defined scopes of authority.

Where existing national registries are incomplete or fragmented, the Commission should establish minimum criteria for issuing credentials to ensure full business coverage. Integration with the EUDI Wallet and trust services under eIDAS should be a baseline requirement. To further support uptake and legal clarity, national authorities should be required to both issue and accept digitally signed, machine-readable credentials within their remit as they do with licences, permits, certificates, registry extracts, etc. Therefore, clear rules must define how these credentials are issued, stored and used, as the widespread availability of trusted public-sector credentials will be key to encouraging private-sector adoption.

In addition, a pan-European mechanism should be established to allow competent authorities to confirm which organisations are authorised to issue sector-specific credentials – such as banks, healthcare providers or accreditation bodies – ensuring cross-border verifiability whilst preserving sectoral oversight.

## Ensure flexibility in implementation and openness to innovation

The EBW should be mandatory for the public sector and for some specific use cases to ensure validity and scale but should also provide for flexibility in terms of deployment. It must support a variety of implementation models – including mobile, enterprise-integrated and cloud-based solutions – and allow participation by qualified public and private providers.

Technical specifications should be based on open, interoperable standards to facilitate integration with existing business systems, particularly for SMEs. The regulatory framework should avoid prescribing architecture or formats, focusing instead on legal effect and interoperability.

Regulation should focus on the trustworthiness and verifiable credentials themselves, rather than on the design or implementation of wallets. This will allow wallet providers – whether apps, enterprise tools or cloud services – to compete on usability, innovation and features without being constrained by rigid regulatory requirements.

## Embed strong security and accountability mechanisms

Given the nature of the information and transactions involved, the EBW must include appropriate safeguards to prevent fraud, ensure data integrity and enable traceability. Authentication mechanisms, access controls and audit logs should be standard features. Unlike wallets for natural persons, unlinkability is not suitable in the business context – accountability requires that credentials and actions be attributable to legal representatives and thus to the represented legal person. Risk-based implementation should apply, but minimum requirements for assurance and verification should be established at EU level.

## Enable international interoperability and scalable data standards

The EBW should be built to operate not only within the Single Market, but also in alignment with international frameworks to be resilient and future proof. Many European businesses operate globally and need solutions that can interconnect with third-country systems. Compatibility with global identifiers (e.g. LEI), standardised interoperable data formats and internationally recognised credentials will be essential to ensure long-term relevance and usability. The wallet should also support machine-readable, semantically aligned data to enable automation, analytics and cross-system integration.

FOR MORE INFORMATION, PLEASE CONTACT:

Tzvetoslav Mitev

**Director for Data Economy & Public Administration Policy**

[tzvetoslav.mitev@digitaleurope.org](mailto:tzvetoslav.mitev@digitaleurope.org) / +32 494 10 65 82

---

Beatrice Ericson

**Manager for Data Economy, Privacy & Public Administration**

[beatrice.ericson@digitaleurope.org](mailto:beatrice.ericson@digitaleurope.org) / +32 490 44 35 66

---

Alicia Martinez Rodriguez

**Policy Officer for Data Economy**

[alicia.martinez@digitaleurope.org](mailto:alicia.martinez@digitaleurope.org) / +32 494 10 36 29

## About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes corporations which are global leaders in their field of activity, as well as national trade associations from across Europe.