WHITEPAPER

DIGITAL SOVEREIGNTY FOR EUROPE

Why Offline AI Is No Longer Optional and How CABOLO®'s Secure, On-Premises Solutions Align with Europe's Strategic Autonomy in the Digital Age

cabolo®

2026

TABLE OF CONTENTS

Executive Summary	pg 03
The European Challenge	pg 04
The Four Pillars of Concern	pg 05
Where CABOLO® Fits In	pg 06
Cybersecurity Without Compromise	pg 07
Beyond Compliance: A Strategic Choice	pg 08
Looking Ahead	pg 09
About CABOLO®	pg 10

Disclaimer: This white paper explores how the European Union's quest for digital sovereignty, articulated in the European Parliamentary Research Service briefing of the same name, aligns with the architectural principles behind CABOLO®'s offline, AI-powered speech technologies.

Executive Summary

Europe is at a turning point. For the better part of a decade, policymakers in Brussels, Berlin, Paris and Rome have been raising the alarm about a quiet but consequential shift: citizens, businesses and governments across the European Union are gradually losing control over their data, their capacity for innovation and their ability to enforce the laws they themselves have written. The response to this concern now has a name, digital sovereignty, and it is shaping the policy agenda of the entire continent.

The European Parliamentary Research Service (EPRS) briefing Digital sovereignty for Europe sets out the challenge in stark terms. It describes an EU that leads the world in setting ethical standards yet lags behind the United States and China in private investment, patent filings, data collection and the adoption of frontier technologies such as artificial intelligence, quantum computing and the cloud. The briefing makes the case for a new policy approach, one that protects European values while equipping European organisations with the tools to compete and innovate on their own terms.

At CABOLO®, we believe this is precisely the moment where technology providers must step forward with solutions that are not merely compliant, but sovereign by design. Our offline, AI-powered speech technologies are built for exactly the environment the EPRS paper describes: one in which data protection, cybersecurity, resilience, and independence from foreign infrastructure are no longer aspirations, but requirements.

The European Challenge

Digital sovereignty, in its own words

The EPRS paper identifies several interconnected concerns that now sit at the heart of the European digital policy debate. Taken together, they describe a continent that wants to remain open and interoperable with the wider world while also protecting its citizens, its institutions and its competitive future. It is, in other words, a call for technology that keeps data in Europe, in European hands, under European rules, without sacrificing performance or usability.

For solution providers serving the public sector, regulated industries and defence, this is not a distant regulatory conversation. It is a concrete set of procurement, architectural and operational expectations that will shape purchasing decisions across the Union for years to come.

"Citizens, businesses and Member States of the European Union are gradually losing control over their data, over their capacity for innovation, and over their ability to shape and enforce legislation in the digital environment."

— EPRS, Digital Sovereignty for Europe, July 2020

The Four Pillars of Concern

The EPRS briefing converges on four intertwined areas of concern. Understanding each is essential for any organisation designing a sovereign digital strategy.

1. Data Dependency

The global public cloud market is overwhelmingly dominated by non-European providers, and an often-cited estimate suggests that the vast majority of data generated in the Western world is stored on servers located outside the European Union. Under legislation such as the 2018 US CLOUD Act, foreign law enforcement agencies can, in certain circumstances, compel access to data held by providers under their jurisdiction, even when that data belongs to European citizens, businesses or public authorities.

2. Privacy and the Erosion of User Control

The General Data Protection Regulation has made the EU a global standard-setter, and many non-European jurisdictions and multinationals have aligned their practices with it. Yet the economic model of large technology platforms remains built on the extraction and exploitation of personal data. As more of everyday life, meetings, consultations, hearings, legal proceedings, moves into digital formats, the risk of inadvertently surrendering sensitive information to third-party cloud services grows accordingly.

3. Cybersecurity and Supply-Chain Risk

The briefing highlights the EU's concern about over-dependence on a small number of foreign equipment suppliers, particularly in critical infrastructure such as 5G. It also notes the sharp rise in cyber-attacks during the coronavirus pandemic and the need for a truly harmonised, and in some cases compulsory, EU-wide cybersecurity certification regime.

4. Innovation Capacity

Europe has world-class AI researchers, a strong industrial base and a large internal market, but it has historically underperformed in translating research into commercial outcomes. The paper calls for public-private partnerships, a large-scale EU research framework and sustained investment in frontier technologies to close the gap.

Where CABOLO® Fits In

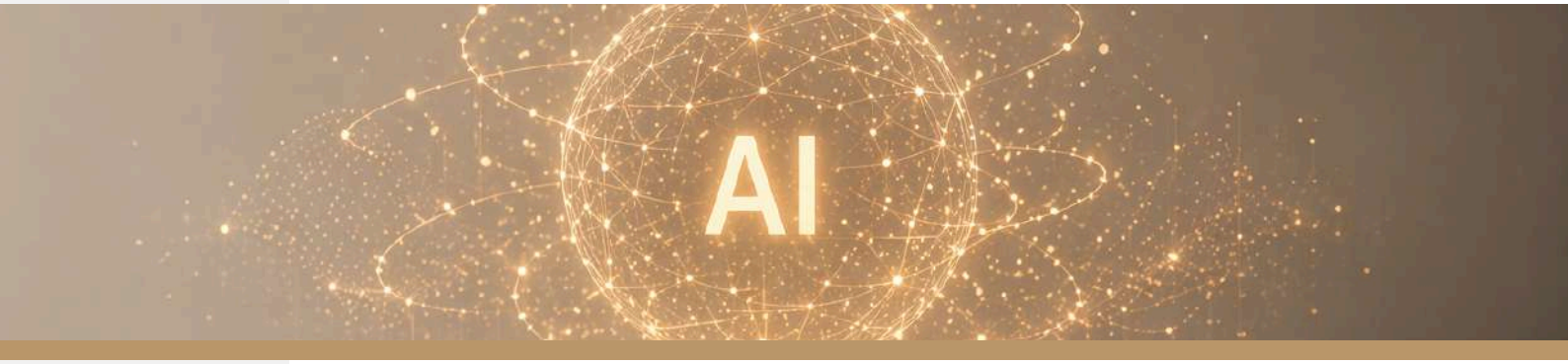
CABOLO®'s solutions were designed from the outset with these principles in mind. We build AI-powered systems that record, transcribe, subtitle, summarise, index, encrypt, and archive speech in real-time, and we do it completely offline, on a dedicated private hardware, with no data ever leaving the customer's environment. That design choice has significant implications when viewed through the lens of the EPRS paper.

Data sovereignty by architecture, not by policy

Because CABOLO® processes audio and video locally on the customer's own device, the question of where data is stored, which foreign legislation applies to it, or which third-party provider might be compelled to disclose it, simply does not arise. There is no cloud inference step, no external API call and no data transit outside the customer's premises. For public authorities, law enforcement agencies, parliamentary bodies, legal professionals, healthcare providers, and defence organisations, this is a meaningful guarantee, not a contractual promise dependent on the behaviour of a distant third party.

Privacy-preserving by design, and GDPR-ready

The EPRS briefing observes that a central challenge for the EU is ensuring that emerging technologies, particularly AI, can thrive without eroding the privacy standards codified in the GDPR. CABOLO®'s offline architecture addresses this tension at its root. Sensitive recordings of confidential meetings, witness interviews, medical consultations and internal board discussions are never exposed to external processing. Combined with AES-256 encryption and support for digital signatures, CABOLO® enables organisations to demonstrate, rather than merely assert, that personal data is being handled in a manner consistent with EU law.



Cybersecurity Without Compromise

The EPRS paper highlights the need for stronger, more harmonised cybersecurity standards across the Union, including the possibility of making EU cybersecurity certification mandatory for key product categories. CABOLO®'s approach, an air-gapped or network-isolated device, robust encryption, and minimal external attack surface, reflects the direction of travel the EU is setting. For customers in sensitive sectors such as government, defence, justice and critical infrastructure, this provides a practical answer to the question of how to adopt AI without widening the cyber threat perimeter.

A European answer for the market demand

CABOLO® is a European solution, developed in Italy, for organisations that operate under regulations. Our speech recognition supports more than 40 languages, reflecting the multilingual reality of the Union itself. Whether it is a committee session in Brussels, a court hearing in Rome, a police interview in Madrid or a board meeting in Berlin, CABOLO® is built to work in the linguistic and regulatory environment that matters to our customers.

This also speaks to the paper's broader industrial ambition: that Europe should not only consume digital technology, but produce it, shape its standards and export its values. By choosing European AI providers for mission-critical workloads, public and private sector buyers contribute directly to the strategic autonomy the EU's institutions have called for.

Sovereignty by architecture, not by policy. European made AI that keeps your data in your hands.

Beyond Compliance: A Strategic Choice

It would be easy to frame digital sovereignty purely as a defensive concept, a matter of avoiding risk, meeting regulatory expectations and ticking boxes. The EPRS paper is clear that it is also, and perhaps more importantly, an offensive one.

Digital sovereignty is about giving European organisations the confidence to innovate, to adopt AI at scale and to build new services without surrendering control over the data that powers them.

For CABOLO®'s customers, this plays out in tangible ways every day:

- Law enforcement agencies transcribe and archive sensitive interviews with complete assurance that no third party has had sight of the material.
- Parliaments and public administrations produce accurate reports of proceedings without routing confidential discussions through external cloud services.
- Enterprises in regulated sectors extract action points and insights from their meetings, calls, and document archives while remaining fully within the bounds of GDPR and sector-specific rules.
- Healthcare providers, use on-device transcription to enhance workplace inclusivity for employees with hearing impairments, without exposing any patient or staff data to external processors.

In each case, the value proposition is the same: the productivity benefits of modern AI, delivered in a form that is consistent with ethical AI values and European law.

Looking Ahead

The EPRS paper closes with a catalogue of concrete initiatives, from a European cloud and data infrastructure to the revision of the e-Privacy Directive, from compulsory cybersecurity certification to new instruments for scrutinising foreign takeovers of high-tech European firms. Taken individually, each is a technical adjustment. Taken together, they describe a continent actively rebuilding its digital foundations.

The role of solution providers in this effort is not to wait for the regulatory architecture to be finalised before acting. It is to offer, here and now, the technologies that make sovereign choices possible. CABOLO® is proud to be part of that effort, and we will continue to invest in offline, secure, European-built AI for the organisations that need it most. Digital sovereignty is no longer a slogan. It is a design principle. And at CABOLO®, it has been ours from the beginning.

About CABOLO®

CABOLO® specialises in offline digital speech processing, text analysis, deep learning, and machine learning. Every year we process millions of hours of events, meetings, speeches, and broadcasts. Our Automatic Speech Recognition (ASR) systems combine Deep Neural Network and Machine Learning methodologies.

Our flagship products, are private-AI powered devices delivering real-time audio-video recording, transcription, subtitling, smart summarisation, indexing, encryption, and archiving of audio, video, and text, all completely offline. It supports more than 40 languages. CABOLO® is already deployed across law enforcement, government, healthcare, legal, higher education, and enterprise environments where privacy, data sovereignty and data security are non-negotiable.

Our linguists, scientists and engineers work to make the most advanced speech intelligence technologies genuinely usable, so that our customers can focus on what matters, and leave the rest to CABOLO®.

Dante® ready ISO 27001 & 42001 Certified eIDAS/eIDAS2 Compliant

Contacts

cabolo.com

info@cabolo.com

Via Poli 29, 10187 Rome Italy

Kings House 36-37, King Street, EC2V 8BB London UK