THE SINGLE MARKET LOVE STORY

10 digital actions to save the 30-year marriage

DIGITALEUROPE

"Today, only 10 out of the top 100 tech companies are European and only 8% of SMEs are trading across one European border."

Foreword

The European single market, a pillar of European unity, stands at a critical juncture. The 30-year marriage needs an urgent revival to keep up with (the digital age). Whilst digital technology fuels economies and solves societal problems, persistent roadblocks within the single market hamper its potential to become a digital powerhouse, as we stated in our recent manifesto. Today, only 10 out of the top 100 tech companies are European and only 8% of SMEs are trading across one European border.

Companies require competences, capital and a common market to take off, but in the digital age they also need scale and speed.

Imagine a unified European AI ecosystem rivalling global giants. Imagine vibrant tech hubs across the continent, not just isolated pockets of innovation. Think of a seamless digital Europe, where data flows freely, nurturing research and development whilst upholding robust cybersecurity. This is the single market we strive for – a digital powerhouse unshackled from the constraints of fragmentation.

The urgency is clear. With inflation, debt and a Recovery Fund set to expire in two years, national budgets alone cannot support our digital ambitions. We need a united front, a renewed push for harmonisation, a rebooted single market fit for the digital age.

Thankfully, the foundation exists. President Delors, thirty years ago, demonstrated that pragmatism can overcome initial doubts. By establishing the single market, he revitalised the European economy.

Today, let's channel that same spirit, overcome existing hurdles, and turn Europe in the next five years into a 'Unicorn Powerhouse.'

Commissioner Breton recognises the digital space as a cornerstone of EU action. We applaud the push for common data spaces, robust cybersecurity and responsible AI development. However, the devil lies in the details. Inconsistent digital laws and fragmented regulations in crucial areas have resulted in a labyrinth of burdens, deterring investors and stifling innovation.

This publication delves into 10 major obstacles – from connectivity to cumbersome AI compliance, disparate data laws and inconsistent procurement rules. We propose clear solutions and a roadmap to fix some of the longstanding structural issues that have plagued the EU's single market for years.

The promise of the single market is one of a prosperous and resilient Europe in turbulent times. Member States need to transcend national borders and build common capacities within critical technologies. Now is the time to walk the talk, to implement, simplify and optimise. It is time to create a stronger united Europe and make it a Digital Powerhouse.

Cecilia Bonefeld-Dahl
Director General
DIGITALEUROPE

Table of Contents

Step 1: Securing capital

Cancer Scan AI's founders – both scientists and engineers – are struggling to get funding for their project. They are facing several challenges, including the fact that there are fewer venture capitalists in Europe and those that exist are excessively cautious when it comes to taking risks.

Getting funding for a new startup is always difficult, but it is especially difficult for startups in Europe. They are 40% less likely than their US counterparts to secure venture capital (VC) funding after five years.

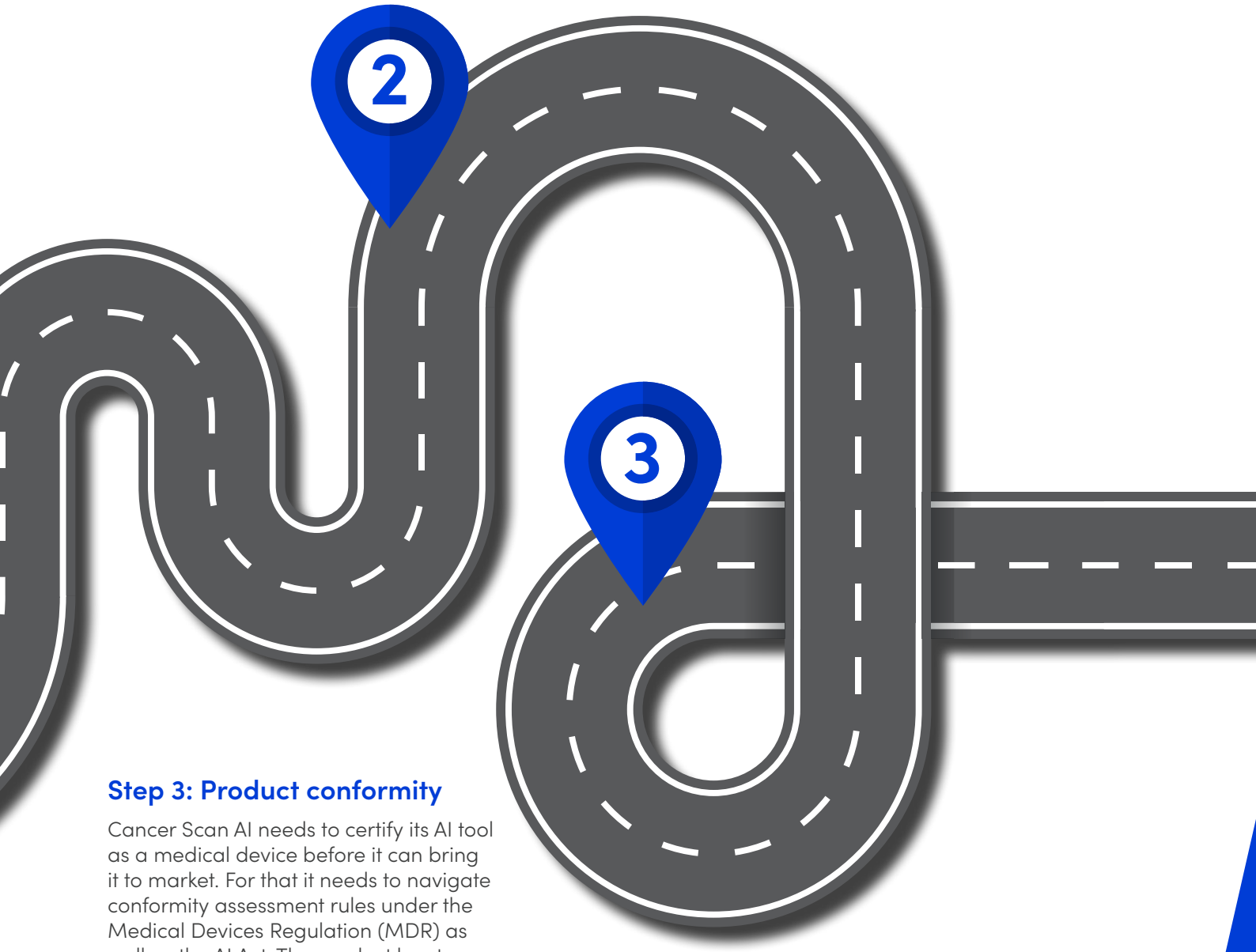
The journey to success from conception to market

Cancer Scan AI is a European medtech startup that is developing a new AI-powered tool for cancer detection. This tool has the potential to save lives by giving doctors a more accurate way to diagnose cancer very early. Take a quick dive into their wobbly journey from fund hunting to bringing their product to market.

Step 2: Product development: Data collection to create algorithm and test AI tool

The Cancer Scan AI team is struggling to access big data sets in Europe to build their algorithm and test their AI tool. 27 different versions of the General Data Protection Regulation (GDPR) applying to health data across Europe do not help, and the upcoming European Health Data Space (EHDS) does not provide much more clarity. Compliance with these 27 sets of rules will pose a massive challenge to Cancer Scan AI when they reach the point of expansion across other countries in Europe.

Data to AI is like fuel to an engine, powering its ability to make informed decisions. Obtaining medical data in Europe is a major challenge due to fragmentation of healthcare systems and to the many strict rules governing data processing (GDPR, EHDS, Data Act, Data Governance Act). Getting permissions can take months if not years and data sets are often incomplete and incompatible, which makes it less useful for training and validating AI models.



Step 3: Product conformity

Cancer Scan AI needs to certify its AI tool as a medical device before it can bring it to market. For that it needs to navigate conformity assessment rules under the Medical Devices Regulation (MDR) as well as the AI Act. The product has to meet a long list of requirements that have not been aligned between regulations.

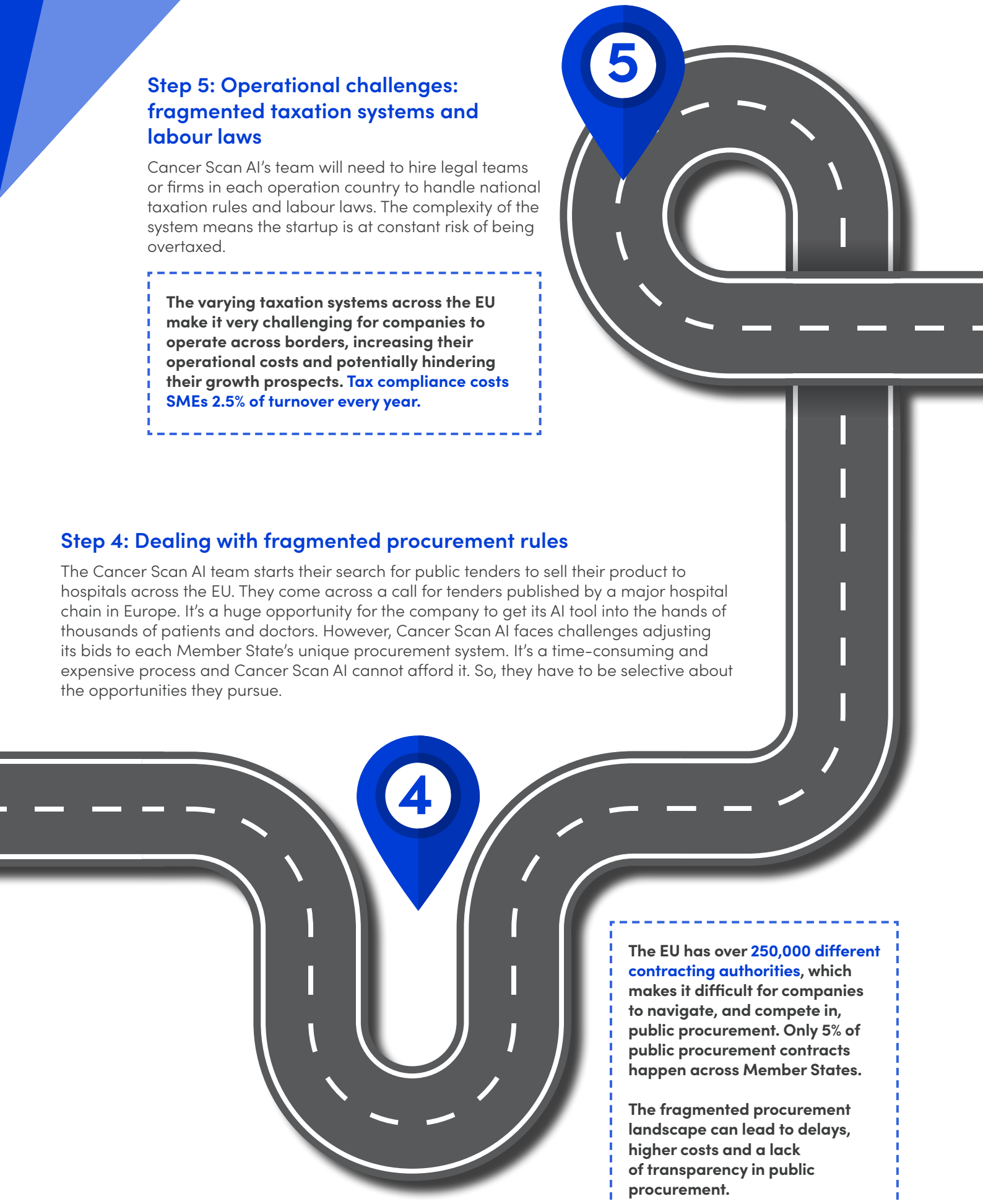
Step 5: Operational challenges: fragmented taxation systems and labour laws

Cancer Scan AI's team will need to hire legal teams or firms in each operation country to handle national taxation rules and labour laws. The complexity of the system means the startup is at constant risk of being overtaxed.

The varying taxation systems across the EU make it very challenging for companies to operate across borders, increasing their operational costs and potentially hindering their growth prospects. Tax compliance costs SMEs 2.5% of turnover every year.

Step 4: Dealing with fragmented procurement rules

The Cancer Scan AI team starts their search for public tenders to sell their product to hospitals across the EU. They come across a call for tenders published by a major hospital chain in Europe. It's a huge opportunity for the company to get its AI tool into the hands of thousands of patients and doctors. However, Cancer Scan AI faces challenges adjusting its bids to each Member State's unique procurement system. It's a time-consuming and expensive process and Cancer Scan AI cannot afford it. So, they have to be selective about the opportunities they pursue.

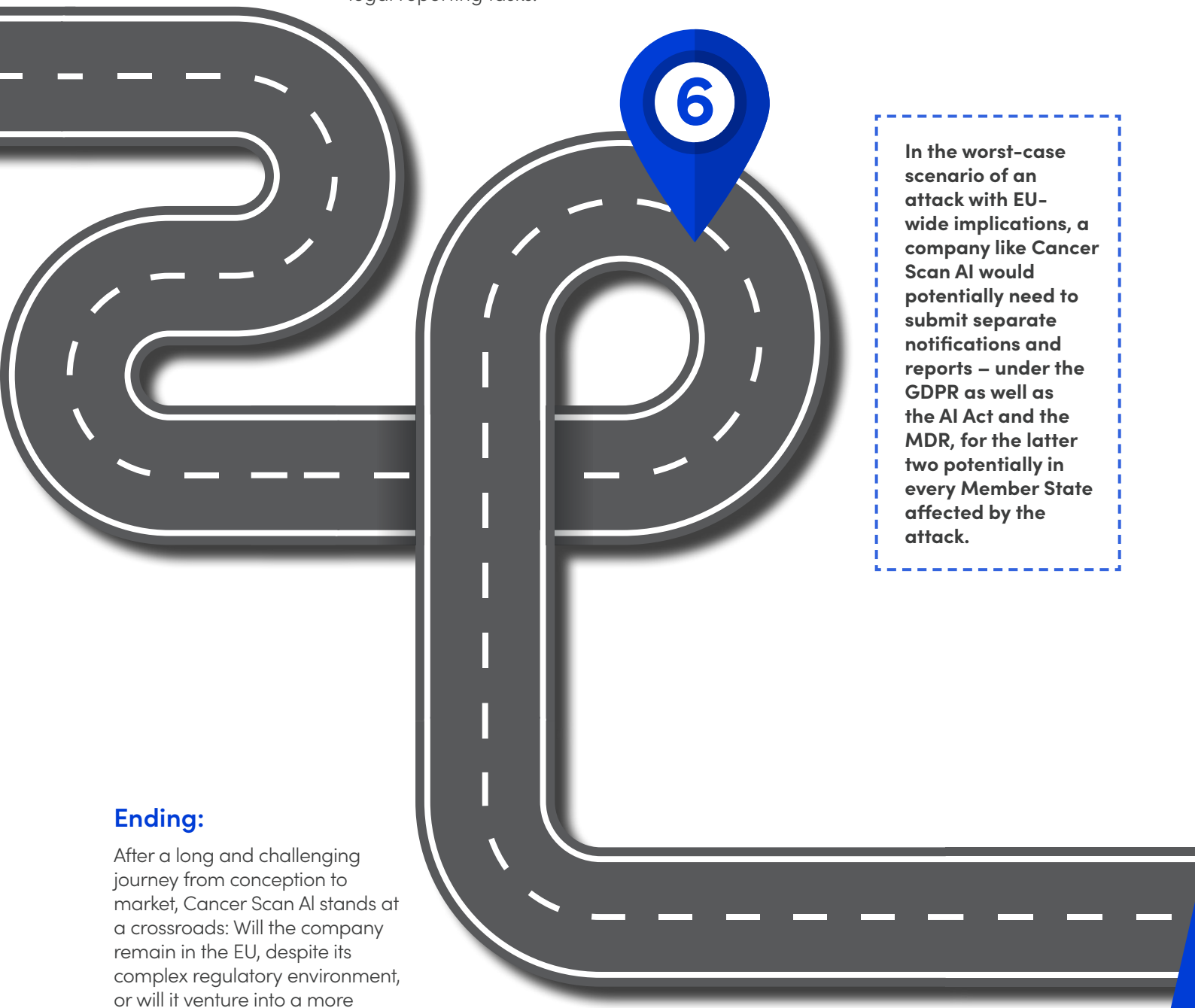


The EU has over 250,000 different contracting authorities, which makes it difficult for companies to navigate, and compete in, public procurement. Only 5% of public procurement contracts happen across Member States.

The fragmented procurement landscape can lead to delays, higher costs and a lack of transparency in public procurement.

Step 6: Handling a crisis – incident reporting

The Cancer Scan AI team is in crisis mode. They've just discovered that they have been hacked, and sensitive patient data has been leaked. They need to act fast to contain the damage and protect their patients' privacy, but they have to face a mountain of incident reporting paperwork towards multiple authorities under the GDPR, the MDR and the AI Act. Instead of focusing on fixing the problem, the Cancer Scan AI team has to mobilise their resources to attend to all the administrative and legal reporting tasks.



In the worst-case scenario of an attack with EU-wide implications, a company like Cancer Scan AI would potentially need to submit separate notifications and reports – under the GDPR as well as the AI Act and the MDR, for the latter two potentially in every Member State affected by the attack.

Ending:

After a long and challenging journey from conception to market, Cancer Scan AI stands at a crossroads: Will the company remain in the EU, despite its complex regulatory environment, or will it venture into a more business-friendly region? Will it continue to scale up or will it fail to survive the competition?

What if Cancer Scan AI were to make the exact same journey in the US?

Step 1:

Securing capital for Cancer Scan AI would be significantly easier in the US compared to Europe, owing to the well-established venture capital culture. Statistics reveal a stark contrast: after 9 years, European startups receive **54%** less private investment than their US counterparts, while a staggering 61% of global AI funding flows into US companies. Conversely, EU start-ups garner a mere **6%** of this funding, highlighting a significant discrepancy in investment opportunities between the two regions.[1]

Step 2:

Data collection should be easier to carry out for Cancer Scan AI in the US as healthcare data interoperability is a **federal** competence whilst the EU relies on **27 different approaches** across Member States.

[1] CEPS, Forge ahead or fall behind: Why we need a United Europe of Artificial Intelligence, available at https://cdn.ceps.eu/wp-content/uploads/2023/11/CEPS-Explainer-2023-13_United-Europe-of-Artificial-Intelligence.pdf

DISCLAIMER

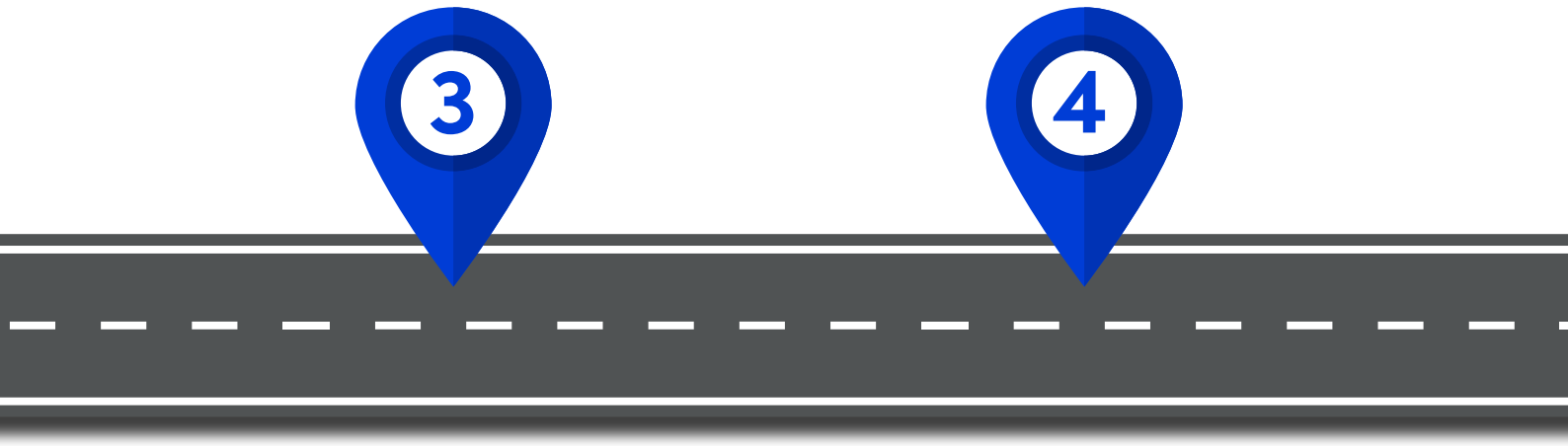
The examples provided are for illustrative purposes only and have been selected to demonstrate indicative points of stark between the US and EU contexts.

Step 3:

Product certification in the US generally takes less time than in the EU. On average, it would take Cancer Scan AI about **5 months** to get its AI product certified in the US versus **1.4 years** in the EU without counting the upcoming AI Act issues.[2]

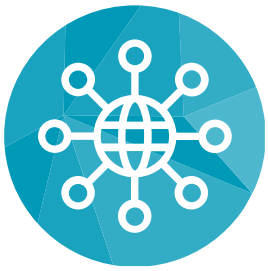
Step 4:

Procurement rules are more straightforward in the US. Contrary to the EU, the US has a **single** reimbursement system with nation-wide decisions on medtech device classification and level of coverage requested.



[2] Calculations based on Gesundheit Österreich GmbH, Monitoring the Availability of Medical Devices and In Vitro Diagnostic Medical Devices in the EU, available at https://app.powerbi.com/view?r=eyJrIjoiNGYyMDU3NmQtYjY3Yy00YzMxLThkYmEtNTUyNDQ0ZGY-wNWY5IiwidCI6ImIyNGM4YjA2LTUyMmMtNDZmZS05MDgwLTcwOTI2ZjhkZGRiMSIsImMiOjh9%20
and Hardian Health, How long does an FDA 510(k) submission for SaMD and AI actually take?, available at https://www.hardianhealth.com/insights/how-long-does-an-fda-510k-actually-take

The path to a successful single market: 10 roadblocks, 10 quick fixes



1. Connectivity

Europe is too fragmented and slow to attract connectivity investment. Removing these barriers is imperative to achieve gigabit connectivity for everyone and everywhere in the EU by 2030, as recommended in our Manifesto.[3] Re-evaluating the attractiveness of the European market for EU and foreign investors is needed. This has been damaged by poor public funding and a lack of ability for telecoms operators to merge and scale up across Europe. If this fragmentation problem is unresolved, it will impact the ability of infrastructure and service providers to launch offerings at scale, and could even slow down Europe's rollout of 6G technology.

- **Incoherent spectrum allocation:** The EU's attempt to harmonise spectrum allocation has been only partially effective. The European Electronic Communications Code aimed to unify this process, but inconsistencies in application by Member States have led to disparate auction timings, prices and licence lengths across Member States. 69% of connectivity experts view spectrum auction delays as a key hurdle to Europe's network leadership.[4]

There are also disjointed approaches across the EU to making the spectrum available. All this fragmentation means market strategies and infrastructure plans must be individualised for each market segment, which increases operational expenditure to cope with greater legal complexity.

RECOMMENDATION

Strengthen spectrum harmonisation in Europe. Member States and the Commission should improve coordination of binding decisions at European level to boost private investment impact.

[3] Europe 2030: A Digital Powerhouse. DIGITALEUROPE's manifesto for the next Commission, available at https://www.digitaleurope.org/resources/europe-2030-a-digital-powerhouse-digitaleuropes-manifesto-for-the-next-commission/
[4] DIGITALEUROPE, Mind the Gap: A new Connectivity Act for the Digital Decade, available at https://www.digitaleurope.org/resources/mind-the-gap-a-new-connectivity-act-for-the-digital-decade/

- **Inconsistent network infrastructure policies:** Europe is supposed to have common rules already in place to facilitate the rollout of high-speed electronic communications.[5] Their implementation has, however, stumbled because competencies in areas like permitting are spread amongst too many public bodies with competing goals. This is especially the case in federal Member States. The result is a process for deploying broadband bogged down by a labyrinth of procedures that slow down broadband deployment.

RECOMMENDATION

Uniformly roll out an ambitious Gigabit Infrastructure Act across the EU,[6] with easy access to public infrastructure and a single contact point in each Member State.

- **Legal ambiguity on advanced 5G services like network slicing:** The interpretation of the Open Internet Regulation has been prone to excessive divergence by various Member States,[7] which has deterred specialised 5G services for companies operating in specific verticals.

RECOMMENDATION

Issue unambiguous guidance on compliance for specialised services under the Open Internet Regulation.

[5] Broadband Cost Reduction Directive (Directive 2014/61).
[6] COM(2023) 94 final.
[7] Open Internet Regulation (Regulation (EU) 2015/2120).

2. Unlocking venture capital investment

Europe's innovators face a systemic struggle to find investments for growth in the absence of a Capital Markets Union (CMU) that fosters larger and risk-ready investment funds. Other temporary options building on InvestEU are also notably absent. European startups get less than 60% of the venture capital funds of their US peers.[8] And in a ranking of OECD countries for startup founder appeal, less than one-third of the top 15 are from the EU.[9] When they turn into scale-ups, this divide only deepens.[10] The US market almost always becomes the go-to for European firms needing over €50 million. This funding gap is critical and should concern everyone: Europe's green and digital transitions require a combined additional investment of €745 billion each year.[11]

The CMU could meet a significant chunk of this demand and help plug this investment gap. It could also be an occasion to simplify the process for companies to launch on the stock market, which in some Member States requires daunting documents that can stretch to 800 pages.[12]

RECOMMENDATION

Speed up the creation of late-stage investment vehicles; transition towards one set of EU rules for all national capital markets supported by more cooperation between local and EU authorities.

[8] European Investment Bank, From starting to scaling How to foster startup growth in Europe, available at https://www.eib.org/attachments/efs/from_starting_to_scaling_en.pdf
[9] OECD, Talent Attractiveness 2023, available at https://www.oecd.org/migration/talent-attractiveness/research-and-methodology.htm
[10] Sifted, Unicorn drain: Europe is still losing its most valuable startups to the US, available at https://sifted.eu/articles/european-unicorns-relocating-us
[11] European Commission, Strategic Foresight Rpoer 2023, available at https://commission.europa.eu/system/files/2023-07/SFR-23-beautified-version_en_0.pdf
[12] Oxera, Wie können Börsengänge für Startups in Deutschland erleichtert werden? Internationaler Vergleich und Handlungsempfehlungen, available at www.bmwk.de/Redaktion/DE/Publikationen/Studien/studie-wie-koennen-boersengaenge-fuer-startups-in-deutschland-erleichtert-werden.pdf?__blob=publicationFile&v=6#:~:text=und%20B%C3%B6rseng%C3%A4nge%20von%20Start%2Dups%20in%20Deutschland,-Gut%20funktionierende%20%C3%B6ffentliche&text=Wachsende%20Unternehmen%20nutzen%20den%20Markt,und%20ihr%20Profil%20zu%20sch%C3%A4rfen

3. Artificial intelligence in health

The introduction of the AI Act will create regulatory confusion in the health ecosystem in concrete operations such as AI model training, development and testing, as well as AI incident reporting. It will layer atop the existing Medical Device Regulations,[13] which already strictly govern AI-infused medical technologies.

- **Duplicative compliance processes in product development: The Cancer Scan AI fictious example used at the beginning of this publication demonstrates the hardships faced by tech innovators in the healthcare sector.** From stringent requirements under the MDR to new implementation guidance, standards, reporting tools and procedures under the upcoming AI Act,[14] the regulatory burden is real. Companies would need to invest in legal expertise and consulting, and collaborate with a notified body to navigate the AI Act and MDR. Its own interpretation of requirements, which may differ from others', will guide the product development process. This means delays will extend the current, already long 12-24 month certification period for such type of systems. Notified body costs will exceed the €250,000 for a 5-year cycle now needed for a firm with a single AI-based medical device.[15]

Even when it is over, companies will still face the daunting challenge of explaining to hospitals, investors and potential customers the nuanced risk profile of their AI diagnostic tools. Even worse, they will need to cope with the constant fear of legal challenges and possible significant fines throughout the compliance phase.

RECOMMENDATION

Create implementing rules recognising that sector-specific governance and enforcement frameworks,[16] like those in the MDR, should be used to assess and apply the AI Act requirements and obligations.

[13] Regulations on Medical Devices (MDR, Regulation (EU) 2017/745) and on In Vitro Diagnostic Devices (Regulation (EU) 2017/746).
[14] COM/2021/206 final.
[15] Internal estimates.
[16] Such frameworks include notified bodies, requirements, guidance, standards and tools.

- **Overlapping reporting requirements:** Consider a company in France familiar with the MDR regulatory framework, now deploying AI software to monitor respiratory systems. The company has a long-standing dialogue with ANSM, France's sectoral regulator.[17] The introduction of the AI Act will require it to create an entirely new regulatory dialogue from scratch with the future competent authority under the AI Act. Two parallel regimes will ensue. Regulatory confusion will be particularly present in areas like incident reporting, given the different definitions of 'serious incident' between MDR and AI Act.[18]

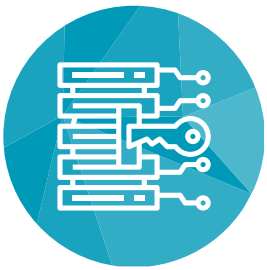
RECOMMENDATION

Follow the principle of once-only reporting endorsed by the Commission and report to a single designated authority.

"A lot of medical practitioners in Europe are still rather sceptical about the adoption of new technologies in medicine. New technologies are usually implemented into clinical practice in the US first, and only later used in Europe. For example, multigene molecular profiling for precision oncology is now routine in the US, even being covered by Medicare, while in Europe it is mainly performed in large medical centres under research budgets. This issue and Europe's very fragmented market have slowed down the rollout of the Realtime Oncology Treatment Calculator, our AI-based tool which supports oncologists to select the most appropriate molecular-based targeted treatment options for cancer patients."

István Petak
Chief Executive Officer,
Oncompass Medicine

[17] Agence nationale de sécurité du médicament et des produits de santé
[18] For example, the MDR considers the impact on patients, users or others, whilst the AI Act broadly refers to 'a person.'



4. Data economy

THE CASE OF INDUSTRIAL DATA:

- **Fragmented enforcement of business-to-business data sharing:** The Data Act mandates industry-wide data sharing, a move fraught with unpredictable implementation costs.[19] Adding to these, there is a severe risk of fragmented enforcement due to the tangled web of public bodies overseeing its implementation. Such costs and legal confusion could effectively deter, rather than incentivise, Europe's data economy. Under the Data Act, Member States can designate multiple competent authorities for enforcement. These are in addition to data protection authorities under the GDPR[20] as well as other sector-specific bodies, which all maintain their enforcement powers. The setup of the Data Governance Act,[21] with bodies responsible for managing 'data intermediation services' and overseeing 'data altruism organisations,' add to this complexity. We estimate firms may have to navigate interactions with up to a dozen different authorities in each Member State where they operate.

RECOMMENDATION

Clarify that firms are subject to a single lead competent authority under the Data Act.

- **Overlap in business-to-government data sharing:** The Data Act grants statistical offices in the EU the right to access private data for statistical and public interest purposes. The proposed revision of the European Statistics Regulation introduces almost identical data sharing requirements for private companies.[22] It therefore introduces clear risks of redundant data requests from both legal frameworks at EU level, and even from possible extra sectorial rules or future national legislation.

RECOMMENDATION

Recognise the Data Act's primacy as framework governing business-to-government data access for official statistics in the EU.

[19] Regulation (EU) 2023/2854.
[20] Regulation (EU) 2016/679.
[21] Regulation (EU) 2022/868.
[22] COM/2023/402 final.

"The EU from the outside is often seen as a single market, but actually we're still looking at the 27 independent states often with very fragmented laws. It still is often the case that there are some bits and pieces here and there that you have to consider when doing business locally. So, from our side, from a business that is operating globally, we do appreciate first and foremost less fragmentation. Having as uniform a rule as possible is good."

Aleksander Tsuiman, Veriff

THE CASE OF HEALTHCARE:

▶ **Implementation and interpretation of laws:** Picture an EU-based digital health startup, on the brink of breakthrough innovations, yet burdened by the divergent interpretation of the GDPR across Member States. The EHDS could tackle that fragmentation and be a catalyst for progress, offering opportunities to delve into (health) for groundbreaking insights.

RECOMMENDATION

Ensure a harmonised framework for health data, data protection and privacy, including alignment and consistency between the GDPR and the future EHDS.

▶ **Risks of unclear or fragmented international health data transfer requirements:**

- The GDPR provides strict legal avenues for international transfers of personal (electronic health) data. However, were the EHDS to allow Member States to maintain or introduce further conditions, including data storage requirements and limitations for international transfers of, and access to, personal electronic health data, adverse effects would emerge on international health research and innovation (R&I) collaborations, pan-European medical registries and ubiquitous digital health services.[23]
- The EHDS provisions on international transfers of non-personal/anonymous electronic health data would lead to significant implementation problems due to the lack of clarity over what would constitute 'non-personal/ anonymous electronic health data.'

RECOMMENDATION

Aim for harmonisation between EHDS and GDPR and refrain from introducing in the EHDS new data localisation provisions or international health data transfer restrictions. Also, clarify the EHDS definition of 'electronic health data' and its subsets.[24]

[23] DIGITALEUROPE, European Health Data Space (EHDS): key issues to address in trilogues, available at https://cdn.digitaleurope.org/uploads/2024/01/EHDS-trilogues-DIGITALEUROPE-position-paper-1.pdf.
[24] Specifically, what constitutes 'non-personal/anonymous electronic health data.'

5. Securing Europe's critical infrastructure: Cybersecurity for regulated entities

The EU's response to the rising tide of cyberattacks has been important and justified over recent years. However, it has also led to an overly crowded regulatory landscape. This complicates the EU's cybersecurity efforts since it dilutes scarce cyber talent across many requirements and institutions. It risks leaving the EU more, not less, vulnerable to escalating cyber threats. The European Court of Auditors has noted the risks of new proposed initiatives in making 'the whole EU cybersecurity galaxy more complex.'[25]

- **Inconsistent compliance rules for software :** Cloud-based software tools will be subject to both the Cyber Resilience Act (CRA) and the NIS2 Regulation,[26] despite these targeting different aspects of the cybersecurity domain. The CRA focuses on cybersecurity in products, whilst NIS2 is about the cybersecurity risk management in operations and services of essential and important entities in Europe. However, most products nowadays are backed by cloud services,[27] creating a blurred line of security requirements applicable to them.

RECOMMENDATION

Issue guidance clarifying the interplay between NIS2 and CRA for remote data processing services.

[25] European Court of Auditors, Opinion 02/2023, available at https://www.eca.europa.eu/ECAPublications/OP-2023-02/OP-2023-02_EN.pdf.
[26] COM/2022/454 final and Directive (EU) 2022/2555, respectively.
[27] These can be software-as-a-service (SaaS) solutions covered under NIS2 and also qualifying as 'remote data processing' under the CRA.

▶ Duplicative reporting

- Financial services: DORA is supposed to take precedence for cybersecurity risk management of financial services institutions specifically.[28] Yet, this not necessarily the case on incident reporting. After filing an initial incident notification, a bank may have to submit subsequent reports about the same cyberattack not just to various national authorities responsible under DORA, but potentially also to Member State computer security incident response teams (CSIRTs) if authorities deem this justified. At a time when quick action is essential, this double layer of reporting diverts staff from swiftly responding to the cyberattack itself to managing paperwork and compliance.

- Personal vs non-personal data: Whilst cybersecurity regulations such as CRA and NIS2 focus on the stability and resilience of networks, systems and products, the GDPR requires a distinct notification process for personal data breaches.

This duality forces entities to navigate parallel reporting routes for what is essentially a single cybersecurity event with privacy implications. Take the case of a European manufacturer of industrial pumps. It primarily handles industrial data, but it qualifies as a controller of personal data, namely customer information, under the GDPR. The manufacturer faces a cybersecurity breach that compromises such customer data. It must undertake the meticulous process of reporting the incident to the competent CSIRT in the EU whilst, concurrently, reporting the personal data breach to the competent data protection authority (DPA) under the GDPR.

RECOMMENDATION

Follow the principle of once-only reporting endorsed by the Commission and report to a single designated authority.

[28] Regulation (EU) 2022/2554.

- **Consolidating cybersecurity bodies:** The landscape of cybersecurity authorities in EU legislation has evolved significantly. ENISA, established two decades ago, laid the foundation of EU action. With the 2016 NIS Directive,[29] all Member States established their cyber authorities, including CSIRTs, and a Cooperation Group and CSIRTs Network were formed at EU level. The European Cybersecurity Competence Centre emerged to bolster capabilities. EU-CyCLONe aimed at fostering cooperation during major cyber incidents. The recently proposed Cyber Solidarity Act would establish a European Cyber Shield to connect Member State Security Operations Centres (SOCs) and a Cybersecurity Emergency Mechanism for recovery.[30] This multifaceted approach has introduced a complex network of entities.

RECOMMENDATION

Consolidate cybersecurity entities to enhance operational efficiency and better support the resilience of critical infrastructure like energy grids.

- **Absence of cybersecurity certification schemes:** The Cybersecurity Act was intended to create greater harmonisation of cybersecurity requirements via the introduction of cybersecurity certification schemes.[31] As the regulatory landscape has developed, these schemes grow in importance as key ways of demonstrating compliance. These schemes have not been adopted quickly enough. As a result, companies looking to serve multiple European markets are forced to pursue multiple national certifications, adding costs and fragmenting access across the Single Market.[32]

RECOMMENDATION

Agree a clear timetable for the development and approval of EU certification schemes and ensure that these schemes are modelled exclusively around technical cybersecurity safeguards.

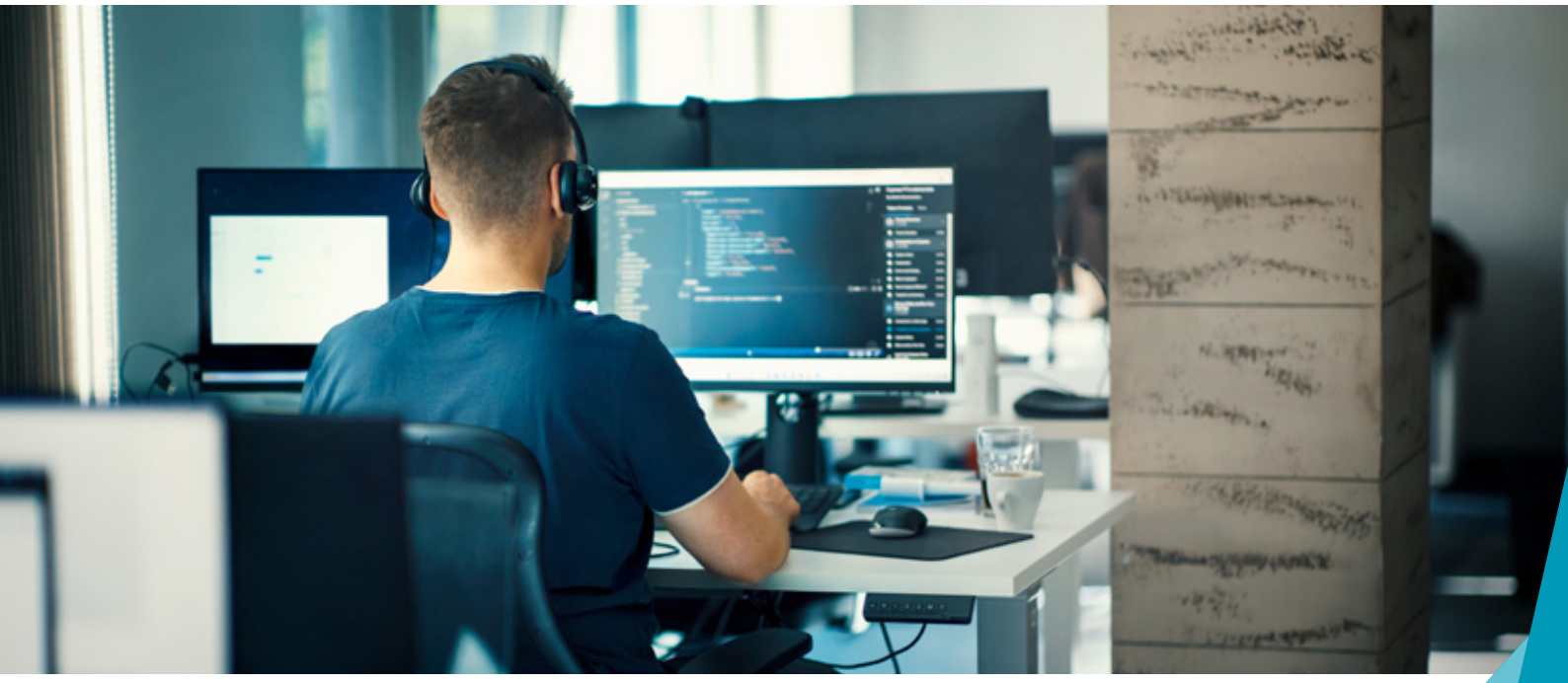
[29] Directive (EU) 2016/1148, now succeeded by NIS2.
[30] COM(2023) 209 final.
[31] Regulation (EU) 2019/881.
[32] DIGITALEUROPE, Adapting ENISA's mandate and collaboration in a changing cyber landscape, available at https://cdn.digitaleurope.org/uploads/2023/09/DIGITALEUROPE_Adapting-ENISAs-mandate-and-collaboration-in-a-changing-cyber-landscape.pdf.

6. European harmonised standards for software

As software regulation intensifies in Europe, there is an escalating risk of a siloed standardisation process to generate European harmonised standards in areas like software, including for risk assessments and testing.[33] Firms risk facing multiple sectorial frameworks, each offering its own variation of similar standards. In areas like software conformance testing, common standards do exist but are limited to critical public safety areas like customs and border control due to an imperative for Member States and EU authorities to actively cooperate.

RECOMMENDATION

Ensure the standardisation process creates standards that are flexible and work across different areas.



[33] Harmonised standards are a specific category of European standards developed by a European standardisation organisation (CEN, CENELEC or ETSI), following a request, known as a 'mandate,' from the European Commission. Companies can use them to prove their products comply with the technical requirements of the relevant EU law.

7. Public procurement of digital services

The Public Procurement Directive allows for too much variation in national implementation and lacks concrete IT procurement guidelines.[34] Digital companies grapple with 27 disparate approaches, which reduce citizens' access to improved public services and hinder business growth through governments acting as buyers. Fragmentation also stifles opportunities for joint procurement by multiple EU countries, which are making some progress in areas like defence.[35] Some Member States have even exceeded the provisions of the Directive. The Netherlands, for instance, mandates cloud service providers to enter into procurement arrangements where the source code or other critical data is placed in the custody of a third party.[36] Language barriers, specific staff requirements and limited information make it further complex for digital firms to tender in other EU countries. Regrettably, proposed laws like the Cyber Solidarity Act cement these problems, asking relevant service providers to deliver in the local language, even if cybersecurity is inherently cross-border in nature.

RECOMMENDATION

Turn the Public Procurement Directive into a Regulation and promote harmonised contract award criteria, valuing cybersecurity and sustainability equally with cost. In the short term, issue guidelines under the Directive for software procurement.

[34] Directive 2014/24/EU.
[35] The EU recently approved EDIRPA, an instrument allowing at least 3 Member States to jointly procure defence solutions.
[36] So-called escrow agreements in procurement language.

8. Finding top talent

Europe faces talent acquisition challenges due to the lack of a real single market for freedom of labour mobility mixed with outdated labour taxation rules.

- **Uncoordinated employee stock option policies:** Europe has a fragmented approach to employee stock options – a mechanism through which companies can offer shares to employees as part of their compensation, and which Europe's scale-ups see as way to compete for tech talent against larger, better resourced peers. Some Member States like Estonia and Latvia support fully stock option pools, whilst others have more restrictive or outdated legislation hampering this practice through heavy taxation.[37] The lack of a single, EU-wide employee stock ownership framework means SMEs operating in multiple Member States are blocked from offering universally recognised stock options to existing employees and prospective hires. This fragmentation amounts to a hiring restriction at a time when ICT specialists are just 4.6% of Europe's workforce. There is a need to urgently build upon the Commission's two-year-old announcement of a Working Group on employee stock options under the European Innovation Council Forum.[38]

RECOMMENDATION

Create an EU-wide employee stock option law before 2026.

[37] In Romania, for instance, employee stock option provisions date back to 1990. Index Venture, Not Optional Ranking, available at https://www.notoptional.eu/en/country-ranking.
[38] COM(2022)332.

- **Disjointed framework on hiring of third-country nationals:** The EU attracts 31% of all highly skilled third-country nationals choosing to work in an OECD country.[39] Europe misses a common EU-wide policy on hiring highly skilled talent from third countries that would bolster its standing amongst peers. Most Member States implement uncoordinated labour market tests (LMTs), forcing employers to prove they could not find suitable local or EU workers before hiring from outside. These LMTs tend be restrictive and burdening on companies, requiring them, for instance, to update public employment agencies at multiple steps of the hiring process. The 2021 EU Blue Card revision did little to harmonise and streamline LMTs. It still allows individual Member States to enforce these tests during the first 12 months of employing a skilled worker,[40] and to repeat them when it moves to a second EU country.

RECOMMENDATION

Introduce an EU-wide law to streamline EU entry for skilled talent like IT professionals, replacing fragmented LMTs across countries.

- **Unclear recognition of educational qualifications and credentials:** 60% of EU digital firms face a shortage of skilled ICT workers.[41] Several Member States struggle with recruiting IT teachers, no matter the IT curriculum's maturity. This is partially because qualifications and credentials acquired in one Member State are not recognised in another. This challenge is not limited to formal degrees. It also extends to industry-led training, despite these potentially serving as a 'common currency' in the EU IT job market. This market failure hinders the swift integration of ICT talents into digital roles. In some Member States, professions like IT, electromechanical engineering or teaching are regulated, requiring the host country to assess and approve the qualifications of professionals from another Member State before they can work there.[42]

RECOMMENDATION

Create an interoperable European skills passport for mutual recognition of qualifications and credentials, facilitated by digital archiving policies for easier record-keeping in schools and universities; reduce the number of regulated professions in Europe.

[39] OECD, Europe is underachieving in the global competition for talent, available at https://web-archive.oecd.org/2016-06-07/404982-europe-is-underachieving-in-the-global-competition-for-talent.htm.
[40] In circumstances where their labour market situation undergoes serious disturbances such as a high level of unemployment in a given occupation or sector.
[41] Eurostat, Enterprises employing, recruiting and having hard-to-fill vacancies for ICT specialists by economic activity, EU, available at https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Enterprises_employing,_recruiting_and_having_hard-to-fill_vacancies_for_ICT_specialists_by_economic_activity,_EU,_2022.png.
[42] European Commission, Regulated Professions Database, available at https://ec.europa.eu/growth/tools-databases/regprof/professions/generic.

"The biggest opportunities for an SME such as ours are joint R&D funding and joint digital skills training initiatives (in our case, in medical education). Through the application of R&D, companies strive for the development, design and improvement of their products, services and technologies. In addition to creating new products and developing old ones, investing in R&D connects different parts of a company's strategy and business plan, such as marketing and cost reduction. At present, technological development is essential for an SME, so acquiring any new digital skill is an investment in the future of SMEs."

Péter Kristóf,
Chief Innovation Officer, YourAnastomosis

9. Taxation rules

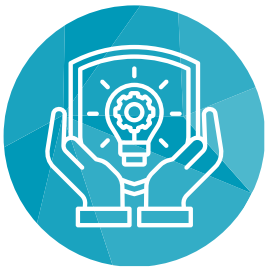
Small firms in the EU often pay up to 30% of their taxes just to handle tax paperwork.[43] This is due to the fragmentation of EU tax compliance, with each Member State defining different tax provisions and interpreting internationally agreed standards inconsistently. This creates uncertainty and poses investment barriers. It happens at a time when clear tax rules and targeted tax incentives are vital to bolster competitiveness. Startups seeking scale need to learn and follow a new set of rules for every country they seek to expand in. There is a real need to foster interoperability between Member States' national tax systems and digitalise many reporting elements, including invoicing. Real-time economy (RTE) initiatives in countries like Finland and Estonia can offer guidance on achieving more digital e-government services.

- **Burdening documentation for social security and labour mobility:** There are rules in place aiming to guarantee coordination of social security systems in the EU, including in case of workers being temporarily sent abroad to work.[44] Firms need to notify authorities before sending workers abroad. This includes filling paperwork to prove the worker's home country social security affiliation. This labour mobility system based on the Posting of Workers Directive is essentially broken now.[45] Germany's staggering expense of €16.72 million on paperwork applications in 2019 alone highlights the scale of the problem. Some Member States offer flexibility, whilst others impose severe fines for not having the relevant documentation. This leads to excessive compliance efforts. In France, firms spend almost 1.5 hours for a single declaration today.[46]

RECOMMENDATION

Harmonise compliance documentation across Member States; exempt workers if posted abroad for a brief period.

[43] SWD(2020) 54.
[44] Regulations 883/2004 and 987/2009.
[45] Directive 96/71/EC, as amended by Directive (EU) 2018/957.
[46] Foundation of Family Businesses, Regulatory and financial burdens of EU legislation in four Member States – a comparative study Vol. 2: Burdens arising from the Posting of Workers Directive, available at www.familienunternehmen.de/media/public/pdf/publikationen-studien/studien/Regulatory-and-financial-burdens-of-EU-legislation-in-four-Member-States_Vol2_Stiftung-Familienunternehmen.pdf



10. Intellectual property framework

- **Uncoordinated databases for law enforcement:** Law enforcement, especially customs, rely on a patchwork of different, non-interoperable databases to keep track of information on intellectual property owners, seized counterfeit goods and intelligence. Crucially, they are not using the IP Enforcement Portal made for EU officers, which leads to repeated work and slowdowns for everyone. These problems are compounded by legal ambiguity on what data law enforcement can legally share. This includes sharing within one Member State, across borders and with private investigators, like those focusing on intellectual property or cybercrime.

RECOMMENDATION

Promote a single secure database for law enforcement, or at minimum, interoperability amongst existing ones; clarify the data-sharing and protection framework for law enforcement activities.

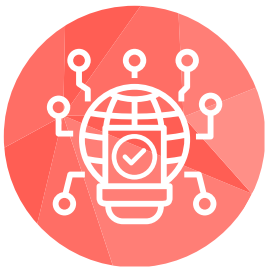
- **Fragmented copyright levies system:** Today's copyright levies system in Europe is a relic of an analogue era. Copyright rules are distorting the Single Market and do not match up with the way people now consume content, mainly through streaming services. Member States' wildly different implementations of the InfoSoc Directive create significant market distortions, preventing the free flow of goods and services.[47] For example, the levies on copy machines are so high in some Member States compared to others that it does not make economic sense to market the machines in those countries.

RECOMMENDATION

Explore a fairer funding model that compensates creators based on current realities and usage behaviour without any market distortion; establish a basic standard to define 'harm,' which is a key source of the current inconsistencies.

[47] Directive 2001/29/EC.

Harmonise, reform, streamline: A three-point roadmap to revitalise the single market



Harmonise rules

Europe's digital pioneers can only thrive in an environment where regulations are stable and consistent. An OECD study shows that moving too quickly from the Commission's impact assessmenta to negotiations prevents Member States from thoroughly analysing legal proposals.[48] Ambiguous legislation can lead to inconsistent implementation across the EU. We believe revamping the way EU lawmaking is done is crucial to effectively protect citizens and provide robust support to businesses. We need:

- **A mandatory 'single market test' to act as a strict legal guardrail for the benefit of the entire EU.** For digital, this must include an emphasis on safeguarding the free flow of data. In the same vein, as guardian of the Treaties, the Commission should be bolder in institutional negotiations and withdraw any proposal if co-legislators are taking stances that would cement fragmentation in the single market.

- **Prioritise regulations instead of directives**, unless national adaptation of EU laws is crucial for industry compliance. Although the GDPR application shows that regulations do not always prevent national discrepancies, they tend to ensure more uniform implementation. Directives often allow Member States to apply the rules too flexibly, leading to no real improvement in market conditions and failure to achieve the intended harmonisation. Sustainability is a key area of fragmented implementation due to the overuse of directives.[49] The Commission should also minimise its use of delegated powers, unless specific technical expertise is needed. This would guarantee that critical subjects remain open to vital public debate and allow industry to prepare its compliance with new requirements.

- **Cite European harmonised standards promptly in the EU's Official Journal (OJEU), and always well before legislation starts to apply.** Key examples are the upcoming AI Act and CRA. Developed with broad market consensus, these standards are key for the functioning of the single market. They help SMEs in particular to comply with legal requirements. Regrettably, their OJEU listing has become increasingly problematic, causing delays for products getting on the market. To complement these efforts, market surveillance authorities should strive for harmonised best practices in enforcing EU digital legislation.

[48] OECD, Better Regulation Practices across the European Union 2022, available at https://www.oecd.org/publications/better-regulation-practices-across-the-european-union-2022-6e4b095d-en.htm
[49] Examples include WEEE, with inconsistent application of so-called Extended Producer Responsibility (EPR) fees where the producer manage product end-of-life. Others include CSRD, CS3D, Green Claims, Directive on empowering consumers for the green transition

- **Annual, formalised 'health check-ups' with industry executives on the ease of business in Europe.** Balanced industry representation must be better engrained in all stages of lawmaking. Current impact assessments fall short in anticipating a law's future complexity, as was the case for the Data Act.

Industry expert forums can complement these assessments by offering actionable insights on proposed legislation. They can also pinpoint positive or negative trends resulting from the impact of specific new policy measures.

Reform EU governance

EU policymakers should no longer be judged by volume of regulatory activity, but by their ability to improve digital competitiveness in Europe. Only 20% of Member States systematically review the impact of adding their own provisions to EU laws, also known as 'gold-plating.' **We recommend the appointment of a dedicated Executive Vice-President for ease of doing business in the next College.** Their targets should be to:

- Cut administrative burden by 50% across the entire stock of EU rules;
- Remove cross-border barriers to reach 30% of SMEs trading across Member States. This would send a strong signal to the business community that Europe is committed to action and measurable progress;
- Boost infringement actions against Member States violating EU-wide rules to protect and improve the single market's integrity. It is important to return to previous higher enforcement levels. Infringement action dropped by a staggering 80% between 2020 and 2023;[50] and
- Launch a platform for 'implementation readiness' for the Commission to guide Member States in effectively transposing and implementing any new law. Examples here are again the AI Act's interaction with sectorial laws and that of the CRA with NIS2 on in-scope software.

A radical revamp of the Commission's governance is necessary to pursue regulatory simplification and harmonisation more robustly and quickly.

[50] Financial Times, Policing of EU market rules drops under von der Leyen's commission, available at https://www.ft.com/content/b81c0d86-4837-42a5-bf01-d4768791f2cf

Streamline reporting and compliance

Regulatory reporting has a legitimate purpose: monitoring adherence to the law. Regrettably, businesses in the EU are undermined by the complexity of the very system meant to oversee them. In areas like cybersecurity, redundant reporting is not just expensive, it also poses its own security risks.

In the short-term, **every Member State should appoint a single reporting authority for all relevant laws**, supported in the long term by an **EU-level one-stop shop** that consolidates all reporting and offers companies the necessary support for compliance. This initiative is not about creating extra bureaucracy. It is about swapping today's multiple existing reporting channels with a single, streamlined process that's better coordinated at European level. It should include the following aspects:

- Single reporting event: Entities report necessary events, like cyber incidents, only once. Criteria for reporting incidents are harmonised across the EU, based on common severity and impact metrics in order to facilitate incident management and response.
- Reporting options: Companies can choose whether to report to their Member State's single reporting authority or to the EU one-stop shop, who should actively collaborate to share information and help solve incidents.
- Government-to-government sharing and no duplicate reporting: The initial reporting authority can share reported data with other authorities where strictly needed. This would avoid repeat requests to the reporting entity.
- Compliance support: The one-stop shop not only serves as a reporting channel but also provides necessary assistance and resources for compliance. This will especially benefit digital SMEs that will need to familiarise with the EU compliance system,[51] which has been mainly applied to physical products and is now being expanded to software in areas like AI and cybersecurity.

The recent Single Digital Gateway, whilst needing to address the inconsistency in Member States' single points of contact, can represent a first step as it can ease access to certain services. It should be the springboard for an ambitious EU one-stop shop in the next Commission term.

[51] So-called New Legislative Framework (NLF).

DIGITALEUROPE represents the voice of digitally transforming industries in Europe. We stand for a regulatory environment that enables businesses to grow and citizens to prosper from the use of digital technologies.

We wish Europe to develop, attract and sustain the world's best digital talents and technology companies.

www.digitaleurope.org

@DIGITALEUROPE

DIGITALEUROPE

DIGITALEUROPE
Rue de la Science, 37
B-1040 Brussels
Info@digitaleurope.org
+32 2 609 53 10