THE EU-SINGAPORE DIGITAL TRADE AGREEMENT: GAMBLING AWAY OUR DIGITAL SOVEREIGNTY

By Javier Ruiz Diaz

GUE/NGL
THE LEFT
IN THE EUROPEAN PARLIAMENT

Author: Javier Ruiz Diaz

Javier Ruiz Diaz is an expert on digital policy and consumer rights, with a focus on areas including digital trade, privacy, AI and platform regulation. He is a member of the UK Government's Trade Advisory Group on Intellectual Property and the Centre for Inclusive Trade Policy, is a former Policy Director at the Open Rights Group and has worked with organisations such as Which?, Public Citizen and Consumers International.

This report was commissioned by Martin Schirdewan, MEP, Co-Chair of THE LEFT in the European Parliament.

Published in October 2025

GUE/NGL
THE LEFT
IN THE EUROPEAN PARLIAMENT

B-1047 Brussels, Belgium
+32 (0)2 283 23 01
left-communications@europarl.europa.eu
www.left.eu

PREFACE

The international trade negotiations landscape has changed dramatically in recent years; what once took decades of careful deliberation now unfolds at unprecedented speed, sometimes without a full understanding of the potential consequences of the rules being negotiated. The European Commission has accelerated its trade agenda, simultaneously pursuing agreements with Mexico, India, Indonesia, Thailand and the Philippines and, most recently, proposing negotiations with the United Arab Emirates. While the Mercosur agreement captures headlines, this broader expansion of trade diplomacy – driven by calls for supply chain diversification and in response to President Trump's tariff war – represents a fundamental shift in approach.

Yet beneath this flurry of trade activity lies a category of agreements that merits far greater scrutiny: digital trade agreements. These instruments address matters that extend well beyond traditional trade concerns, touching the very foundations of how we govern our digital society. This study examines the risks inherent in such agreements, challenges their often overstated benefits, and proposes alternative paths forward.

Our study reveals how the clauses in such trade agreements – particularly those concerning the free flow of data and source code protection – conflict with existing digital legislation and restrict the EU's policy space to regulate the digital sector in the future. We demonstrate that these provisions undermine the EU data protection framework by failing to provide sufficient legal certainty to ensure that sensitive data is kept within the EU. In addition, the study highlights how the digital trade agreement between the EU and Singapore risks weakening workers' rights by reinforcing corporate control over their data. Despite the Commission's assurances to the contrary, we show that this trade deal lacks robust safeguards against tax avoidance, thereby weakening Europe's ability to tax Big Tech effectively.

Our analysis focuses primarily on the digital trade agreement between the EU and Singapore, whose provisions mirror those found in similar digital agreements with Japan and South Korea. While stand-alone digital trade agreements are a relatively recent phenomenon, digital trade clauses were already embedded in agreements with New Zealand and Chile, establishing precedents for future negotiations.

The stakes could not be higher. The Commission estimates that over 60 % of global GDP now involves digital transactions, and Big Tech has grown so powerful it could unfairly dominate markets. This reality prompted significant legislative action within the EU during the previous parliamentary term. Yet these very achievements now face potential erosion through trade agreements that risk undermining the rules that we have worked hard to put in place.

The tension between trade liberalisation and digital regulation extends beyond European borders. The Biden administration's withdrawal from international digital trade negotiations reflected precisely these concerns – a recognition that such agreements could constrain domestic efforts to regulate major technology companies. While the current US administration has adopted a different stance, even characterising EU digital policies as trade barriers, the fundamental challenge remains: how can we ensure that international trade agreements do not undermine democratic oversight of our digital future?

History shows that international trade commitments can limit governments' ability to legislate in the public interest. We must avoid repeating these mistakes in the digital sphere. Our Digital Services Act and Artificial Intelligence Act are hard-won victories for democratic governance of technology. Yet no impact assessment has been conducted on how digital trade agreements might affect this legislation or influence the need for future legislation.

That is why I have commissioned this study – to shed light on the complexities and risks associated with digital trade agreements and foster a more informed debate on this crucial and often contentious area of contemporary trade policy. I am deeply grateful to Javier Ruiz for his exceptional work in preparing this analysis. The questions it raises demand our urgent attention as we navigate the intersection of digital governance and international trade.

Martin Schirdewan
Co-Chair of THE LEFT in the European Parliament

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The EU-Singapore Digital Trade Agreement (EUSDTA), concluded on 25 July 2024, complements the existing EU-Singapore Free Trade Agreement. It governs digital trade in goods and services, covering software, digital media, e-commerce, hardware and a broad range of digital services. While it is promoted as a way to align with the EU's digital trade objectives and boost digital commerce, significant concerns about its potentially negative impacts on EU policy space, digital regulation, data protection, workers' rights, digital industrialisation efforts and taxation remain unaddressed.

SIX KEY RISKS ASSOCIATED WITH THE EUSDTA

- **Reduced policy space to regulate the digital sector in the future**

The agreement's commitments on the free flow of data and restrictions on government access to source code may hinder future regulatory efforts in a rapidly evolving digital landscape. In particular, the provision related to source code could impede AI regulation, as it extends protection beyond traditional software code to cover critical AI components such as training data and model parameters. This effectively creates new intellectual property (IP) protections that restrict regulatory access to increasingly complex AI systems requiring oversight.

- **Conflict with EU digital laws (DSA, DMA, AI Act)**

Provisions that restrict access to source code may weaken the accountability mechanisms of the Digital Services Act (DSA), the Digital Markets Act (DMA), and the AI Act. The extensive investigative powers granted to the European Commission under these laws could be constrained by the limited exceptions in the EUSDTA. For example, the level of scrutiny required by the DMA might not be fully supported by the EUSDTA's exceptions. Similarly, the AI Act's requirement for access to technical documentation – including source code – for conformity assessments could be compromised.

- **Risks to the protection of personal data transferred to Singapore**

The agreement promotes the concept of 'data flows with trust', which may undermine the EU's approach to personal data transfers under the General Data Protection Regulation (GDPR). Although it includes a specific clause safeguarding personal data, the European Data Protection Supervisor (EDPS) has raised concerns about the absence of legally binding language equivalent to the Horizontal Provisions on cross-border data flows and the protection of personal data and privacy adopted by the EU in 2018, creating legal uncertainty and potential conflict with the EU's data protection framework. Singapore's data protection regime is considered less robust than the EU's, with notable deficiencies, such as the exclusion of the private sector from its primary data protection law. There is also a significant risk of onward transfers of EU data from Singapore to countries with inadequate data protection, such as China.

- **Risks to workers' rights**

Provisions concerning data and source code may negatively impact platform workers and the regulation of algorithmic systems in the workplace. A ban on requiring access to source code could hinder the scrutiny of algorithmic management tools, potentially exposing workers to unfair practices. The EU's Platform Work Directive (PWD), which aims to enhance algorithmic transparency and protect workers' rights, may be difficult to enforce if relevant data and algorithms are hosted in Singapore. The agreement also risks entrenching corporate ownership of worker-generated data.

- **Risks to the EU's digital industrialisation goals through a loss of control over data**

The agreement's prohibition on data localisation and its restrictions on mandating specific standards or technologies could undermine the EU's efforts to achieve strategic autonomy in the digital sector and compete globally with the United States and China. While the EU typically argues against data localisation to reduce burdens on businesses, in reality such measures can benefit domestic industries and law enforcement. The EUSDTA's commitments may

conflict with key EU industrial initiatives aimed at fostering European technological capabilities, such as the European Chips Act and the development of common European data spaces.

- **Limitations on the ability to tax technology companies**

Certain provisions in the agreement – such as the ban on customs duties on electronic transactions – could limit the ability of the EU and its Member States to tax international technology companies effectively. Although the EUSFTA contains clauses intended to safeguard the EU's right to introduce tax measures, there are doubts as to whether these exceptions are sufficient to prevent tax avoidance by digital corporations.

DEBUNKING THREE COMMON CLAIMS ABOUT THE BENEFITS OF THE EUSDTA

Claim 1: Digital trade agreements will boost trade in digital goods and services. The European Commission's assumption that digital trade agreements, such as the EUSDTA, will boost trade is not supported by an impact assessment demonstrating this causal link. While regulatory alignment to facilitate data flows could benefit trade, existing agreements, such as the EU's adequacy decisions, already enable significant data exchange without the need for new digital trade agreements. Additionally, supplementary protection of source code lacks an economic justification and could undermine public interest regulations, particularly amid ongoing tensions with the United States over digital regulation.

Claim 2: A ban on data localisation helps SMEs. The European Commission argues that removing data localisation requirements through digital trade agreements would benefit small and medium enterprises (SMEs) by reducing the financial burden imposed upon them. However, in reality, most EU businesses are not required to store data in other countries, and non-EU companies can operate within the EU as long as data transfers meet specific safeguards. The proposed 'data flow with trust' approach, while aiming to streamline data transfer, may actually place a greater burden on SMEs than other mechanisms, such as adequacy decisions.

Claim 3: Disclosure of algorithms will lead to the forced transfer of trade secrets and loss of business value. The report suggests that this concern is overstated, particularly with countries such as Singapore and Korea that have robust intellectual property frameworks and a strong rule of law. It also highlights the fact that the EU is now more likely to require access to the source code of imported software for security reasons. Banning the possibility for governments to require access to source code could potentially create a shadow intellectual property regime, restricting legitimate reverse engineering for interoperability and public interest purposes.

There is strong evidence that the exceptions included in the EUSDTA to protect public policy, workers and consumers are insufficient.

While the agreement includes some language on exceptions in relation to public policy, security, taxation, prudential carve-outs, the right to regulate and source code, it is likely that legal ambiguities and gaps will undermine their practical effectiveness.

- **Ambiguity and narrow scope:** Terms such as 'legitimate public policy objectives' and 'proportionate and targeted access' are ambiguous and open to broad interpretation, which could lead to legal challenges. The exceptions primarily focus on government bodies and courts, overlooking the important role of civil society organisations in the field of oversight. Key risks, especially those related to rapidly evolving technologies, may not be adequately addressed.

- **Weakness of general exceptions:** The right to regulate is a customary right, and its reaffirmation does not prevent lawsuits for violations of the disciplines included in the Singapore agreement. General exceptions, similar to those in WTO law, have historically been difficult to invoke successfully.

- **Concerns regarding the data protection exception.** The EDPS has raised concerns that the modified wording of the personal data protection exception could weaken the EU's ability to protect personal data. The absence of explicit language preserving the full effect of the parties' data protection safeguards further raises concerns about potential challenges under the WTO.

CONCLUSION

The EU is taking a significant gamble with its digital future by relying on complex and untested trade law exceptions to mitigate the substantial risks posed by the EUSDTA.

The EUSDTA, while aiming to promote digital trade, carries significant risks for the EU's regulatory autonomy, data protection standards, workers' rights, and digital industrialisation ambitions. Overall the potential downsides of the EUSDTA outweigh the claimed benefits, and the effectiveness of the built-in safeguards remains highly questionable.

The Commission's over-reliance on exceptions to address the risks of the EUSDTA is problematic because **historically trade exceptions have proven difficult to invoke successfully, and the specific exceptions in this agreement are considered ambiguous, narrow and potentially insufficient to safeguard public policy, workers and consumers**. The effectiveness of the built-in safeguards is therefore highly questionable.

RECOMMENDATIONS

The EU should strive to develop a new EU digital trade approach, including modernising the framework, removing source code restrictions, strengthening data protection through horizontal clauses and adequacy-based transfers, and implementing strategic data localisation carve-outs.

The European Commission should embark on a serious and comprehensive expert assessment that looks at the tensions between digital trade commitments and the regulatory autonomy of the digital economy. It should pause all digital trade negotiations while this analysis is carried out.

1.

THE EU-SINGAPORE DIGITAL TRADE AGREEMENT: WHAT IS AT STAKE?

The EU-Singapore Digital Trade Agreement (EUSDTA) was concluded on 25 July 2024. It complements the broader EU-Singapore free trade agreement that entered into force in 2019.[1] The EUSDTA is in line with the EU's current digital trade policy[2]. The EU concluded a similar agreement with Japan[3] in 2023, and with South Korea in March 2025[4]. The EU also negotiated digital trade clauses in free trade agreements with New Zealand and Chile, and is negotiating with Indonesia, Thailand, the Philippines and Malaysia, among others.

The EUSDTA is also part of a broader EU strategy to build links – including digital partnerships – with the Indo-Pacific region, perceived as the driving force behind global economic growth.[5]

Singapore is a small multi-ethnic nation with a thriving economy, and a key trading hub in South-East Asia. It has signed trade agreements with over 30 trading partners, and over 14 000 European companies have set up their offices/regional hubs in Singapore.[6] This includes well-known businesses such as BMW, Siemens, LEGO and ING insurance, and others such as university ventures, law firms and myriad consultancy and professional services[7]. The 2019 EU-Singapore trade deal has given Singaporean companies access to many economic sectors in the EU[8]. Singapore in turn has opened most service sectors to the EU. Singapore also has many domestic high-tech companies in the fields of finance, green tech or life sciences that could well expand their activities in the EU.[9]

The digital trade agreement contains many different rules that regulate the trade of digital goods and services. The scope of coverage of the agreement is very broad. It covers the trade in products such as software and apps (for example for mobile phones), digital media (films, music, e-books), e-commerce goods (physical goods such as clothes sold via online marketplaces) and digital hardware for smart devices (such as laptops, fridges and cars). It also covers digital services such as e-commerce platforms, streaming services, cloud computing services, telecommunication services, online education, digital marketing and data analytics, to name but a few. This market is already huge, and it is expanding rapidly in Europe[10] and Singapore[11].

Of all the rules contained in the agreement two sets of provisions – on the free flow of data and a ban on requiring access to software source code – are particularly worrying. They create risks for various areas of EU policy without adding any clear value to the specific context of digital trade between the EU and Singapore. These clauses use a formulation similar to that found in other recent EU digital agreements, with some minor differences (see the annex for a detailed comparison).

FREE FLOW OF DATA

The EUSDTA commits the EU and Singapore to **banning policies that may impede the free flow of data. It particularly prohibits governments from demanding 'data localisation'**. This means that the EU may not require Singaporean companies operating in the EU to establish data centres or host their data in Europe, and vice versa.

This affects all digital goods and services transactions between the EU and Singapore, including both personal and industrial data.

The agreement includes a specific provision safeguarding personal data. In 2018 the European Commission committed to including horizontal provisions for cross-border data flows and personal data protection in trade negotiations ('Horizontal Provisions')[12]. However, according to the European Data Protector Supervisor (EDPS), the EU body in charge of ensuring respect for data privacy in the EU, the EUSDTA fails to include the legal wording of the Horizontal Provisions and, in addition, 'creates legal uncertainty as to the Union's position on the

protection of personal data in connection with EU trade agreements and risks creating friction with the EU data protection legal framework.'[13].

Even if the data that is traceable to a person is protected, businesses are particularly interested in accessing data sets and 'meta-data' which they consider crucial in the race for digital industrialisation and innovation. Data is the product of individuals' daily activities either online or in their interaction with smart devices. Companies that already have an established web presence have an in-built advantage with regard to capturing their customers' data. Big Tech companies are keen to maintain that competitive advantage and have therefore advocated for their right to collect, transfer, process and use the data they gain access to without restrictions.

BAN ON REQUIRING ACCESS TO SOFTWARE SOURCE CODE

Another key provision of the EUSDTA is a ban on governments' ability to demand the **'transfer of, or access to, the source code of software'** as a condition for conducting business. The text adds some exceptions, which experts have deemed insufficient.

Source code refers to the written instructions of a computer program and is the foundation of software. Companies, especially Big Tech, are keen to protect source code to maintain their competitive advantage. But access to source code can serve the public interest by enabling researchers to identify biases and allow users to understand how their data is processed.

2.

SIX KEY RISKS OF THE DIGITAL TRADE AGREEMENT WITH SINGAPORE

RISK 1– IT RESTRICTS THE EU'S POLICY SPACE TO REGULATE THE DIGITAL SECTOR IN THE FUTURE

Public concerns regarding digital technologies have changed dramatically in the past ten years, as has the geopolitical context. Digital technologies are evolving too fast and we cannot know today what regulations will be needed in the near future. This new reality stands in direct contrast with commitments included in digital trade agreements to enforce the free flow of data and restrict governments' access to source code. These provisions are designed to protect digital multinationals from governments' efforts to regulate the digital sector and build strategic autonomy.

The main risk inherent in the restriction on access to the source code of software is the potential limitation on the ability to hold digital technologies to account.

The ban on data localisation to protect cross-border data flows may create additional issues for technological accountability. In many situations, regulators will need access to both the source code and the data used to develop or run the system in order to understand its lawfulness or fairness. If that data is not accessible because it has been sent to a different jurisdiction and a trade agreement bans mandatory localisation, this may make regulators' job impossible.

This was made crystal clear by the previous US administration, when it reversed its long-standing approach to digital trade:

'Many countries, including the United States, are examining their approaches to data and source code, and the impact of trade rules in these areas. In order to provide enough policy space for those debates to unfold, the United States has removed its support for proposals that might prejudice or hinder those domestic policy considerations.'[14]

Future regulation of AI

Experts have warned that the ban on requiring access to source code embedded in digital trade agreements such as that with Singapore will hamper the possibilities for future regulation of AI[15].

The House of Lords in the United Kingdom recently concluded a major review of digital trade, where it concluded that:

'The governance of artificial intelligence and its impact on our society and economy is still in its infancy. Regulation of artificial intelligence cannot be undertaken in isolation, and should be considered in cooperation with our global partners. In the light of the mixed evidence that we received, we recommend that the Government undertake a comprehensive review of the use of source code provisions in trade agreements, particularly focusing on the exceptions to the ban on disclosures."'[16]

A key problem is that traditional source code definitions are inadequate for AI systems. While traditional software relies on human-written textual instructions, modern AI systems operate on statistical and mathematical models derived from training data. These models make predictive decisions without explicit programming instructions, making it difficult to identify what constitutes the 'source code' for regulatory or transfer purposes.

The modern scope of source code in AI systems is therefore much broader than in traditional definitions. As demonstrated by Open Source AI[17]frameworks, it encompasses multiple elements: training data, training algorithms, model parameters, statistical information such as weightings, and any other components necessary to reproduce or transfer the technology's functionality.

This means that the ban on requiring access to source code in digital trade agreements is not just protecting what programmers are writing, but the protection is extending to areas that today are not covered by intellectual property laws either at national or international level. Digital trade agreements are introducing legal protection to algorithms through the back door[18].

RISK 2 – THE AGREEMENT WITH SINGAPORE UNDERMINES EXISTING EU DIGITAL LEGISLATION

The European Union has embarked on a major effort not just to regulate technology, but also 'to address the threats stemming from the rise in unaccountable transnational private powers, whose global effects increasingly produce local challenges for constitutional democracies.'[19] Data protection and the GDPR are now complemented by the Digital Services Act (DSA) in an attempt to increase accountability and information asymmetries between individuals and large technology companies. The Digital Markets Act (DMA) approaches these power imbalances from the perspective of competition and market power. Furthermore, the European Union responded to social concerns about artificial intelligence by passing the AI Act in 2024, one of the first major pieces of legislation internationally to ensure that AI systems used in the EU are safe, transparent, traceable, non-discriminatory and environmentally friendly.

What all three pieces of legislation have in common are the EU's efforts to regulate the business practices of large tech platforms.

Experts have warned[20] that the provisions in the EU's DTAs on restricting access to source code could affect the accountability mechanisms of the DSA, DMA and AI Act. Limiting access to source code in DTAs encases technological oversight within the limits set by trade law. In practice, this means that technology governance to respond to social and economic concerns must be squeezed into the exceptions regime in the agreements. This creates a regulatory risk because trade exceptions are notoriously difficult to justify.

The EUSTDA conflicts with the Digital Markets Act (DMA)

Under the DMA, 'gatekeepers' are large digital platforms, such as Google, Amazon, Apple, Meta, and Microsoft, that serve as critical intermediaries in the digital economy. These companies must comply with specific obligations designed to ensure fair competition and prevent abuse of their market power, including transparency requirements, interoperability mandates and data usage restrictions.

The DMA establishes a comprehensive framework of accountability measures that empower the European Commission to regulate gatekeepers. These powers create multiple layers of oversight and enforcement capabilities that require access to technologies. Even if source code is not explicitly mentioned, the level of scrutiny and access required is equivalent.

The Commission can request access to data, algorithms and testing information, and ask for explanations regarding data handling practices and technical operations. The Commission may appoint independent external experts, auditors and officials from national authorities to assist with monitoring and provide specialised expertise. Inspection and audit powers enable the Commission to examine business records in any format and make copies of documents. During inspections, the Commission and its appointed experts can require access to systems and may question staff members.

The Commission has explicitly stated that the EUSDTA is consistent with the DMA, but has not explained the detailed analysis leading to this conclusion. The exceptions included in the agreement with Singapore may not be broad enough to allow competent authorities to carry out the required investigations. The EUSDTA includes a specific exception to 'remedy a violation of competition law', but it appears to cover access only after a problem has occurred. It also includes the possibility of gaining 'proportionate and targeted access' to source code to ensure competition and access to digital markets. The latter may be the most appropriate exception, but it is subject to requirements that may not cover the extensive powers described above.

The Singapore DTA conflicts with the Digital Services Act (DSA)

The DSA establishes a comprehensive framework of accountability measures that empower European regulators, both at national and EU level, to oversee very large online platforms (VLOPs) and very large online search engines (VLOSEs). These are digital services that reach at least 45 million active EU users a month and are subject to enhanced regulatory obligations under the DSA on account of their exceptionally large impact on the digital economy and society. These providers must conduct risk assessments, undergo independent audits and provide data access to researchers and regulators because their scale creates heightened systemic risks to information integrity and consumer protection.

National regulators and the Commission possess significant investigative powers, including the ability to require information from providers and related parties. During inspections, authorities can require explanations about organisation, functioning, IT systems, algorithms and data-handling practices. Providers must explain the design, logic, functioning and testing of their algorithmic systems upon request.

The DSA gives regulators fewer powers to access technologies than the DMA, but the issues covered are broader, generally covering the scope of public interest objectives. In addition, these powers of access can be applied by national entities as well as by the European Commission, and can nevertheless be used to demand access to core aspects of the technology.

The ban on requiring disclosure of source code could impinge on the power of EU regulatory authorities to investigate DSA cases. The Commission has not yet explained how the exceptions included in the DTA overcome the conflict between the objectives of these pieces of legislation and the problematic clauses contained in the agreement.

The Singapore DTA conflicts with the Artificial Intelligence Act (AI Act)

The EU AI Act divides the AI system into four categories following a risk-based approach that focuses on preventing harms caused by high-risk AI systems.

The bulk of the regulation focuses on high-risk AI systems that can have a significant impact on the user, such as profiling tools. Those providing or deploying these systems must create and maintain technical documentation. Some systems must also be checked against various requirements in conformity assessments. Authorities can demand to see these documents. A subset of high-risk AI systems also require an impact assessment to determine their potential impact on fundamental rights.

The AI Act gives powers to the regulators responsible for high-risk systems to demand access to any technical documents. These include relevant data sets, and crucially for the DTA, source code necessary to assess conformity. The European Commission can conduct further in-depth technical evaluations if needed.

The Commission has stated that the exceptions in the digital trade agreement with Singapore enable access to technologies for regulatory purposes, but it has not explained how this would work in detail.[21] The Commission should provide more details on how DTAs are consistent with existing Union policies under Article 207(3) TFEU.

It is worth noting that Singapore has invested heavily in the development and use of AI for government[22] and businesses and is positioning itself as a global AI hub[23]. However, when it comes to AI regulation, Singapore and the EU are on opposite side of the spectrum'. Singapore's model of AI governance has been described as 'light touched'[24]. There are no specific laws or binding rules that directly regulate AI, only sectoral and voluntary frameworks.[25] Singapore's plans for improving AI accountability are not in line with the requirements of the EU AI Act[26].

RISK 3 – EUROPE'S PERSONAL DATA PROTECTION FRAMEWORK IS AT RISK

The EU has an agreed set of standard clauses for use in digital trade agreements designed to protect the GDPR[27]. However, the latest EU DTAs with Japan, Korea and Singapore promote the concept of *data flows with trust*, which could undermine the overall EU approach to personal data flows.

This approach, introduced by Japan[28], focuses on respecting legal regimes while supporting digital trade.[29] The essential element here is to build interoperability among data regimes through 'transfer mechanisms that allow a trusted flow of personal information to third countries, even under circumstances where jurisdictions do not offer similar levels of protection'.[30]

Finding ways to make EU data governance regimes work with other jurisdictions with less robust regimes such as Singapore without imposing European norms and values is a worthy aim. Unfortunately, the data flows with trust concept might create a minimum common denominator approach to data governance that runs counter to the basic assumptions of EU data protection. At present, any EU tools for personal data transfers – such as contracts or certifications – must guarantee that EU levels of protection are maintained when data travels out of Europe.

Singapore is far from having the same standards as the EU in terms of data protection. Changes to Singapore's legal framework for data protection in 2021 brought it closer to the GDPR, but substantive shortcomings remain, including the fact that the main data protection law excludes the private sector. Freedom House, an organisation dedicated to promoting democracy and human rights, assesses Singapore as being 'partially free', finding that the legal framework 'limits freedoms of expression, assembly, and association'.[31]

The digital sector accounts for more than 17 % of its economy[32], and Singapore has the highest rate per capita of venture capital in the world, above the United States, Estonia and Israel.[33] The country also hosts over 100 data centres, including Google's, connected to the world by 24 submarine data cables.[34] Chinese giant tech companies looking for overseas markets have their foreign base there, including Alibaba, Tencent and TikTok/Bytedance.[35] South-East Asia is perceived as the leading market for cloud computing.[36]

The main privacy risk of data flows to Singapore is that some of those companies will then send EU data to other countries without adequate safeguards, in particular China. Despite the development of increasingly sophisticated digital regulation in China, concerns about state surveillance remain, and the prospect of free data flows with the EU remains elusive.[37]

Commitments in the DTA to promoting further regulatory cooperation and mutual recognition of certifications could be abused to facilitate onward transfers. The Singapore Data Protection Trustmark (DPTM) is implemented by dozens of companies, including Chinese behemoths Alibaba, Huawei and Tencent.

Another risk is that Singapore is very active in developing digital trade agreements, having already concluded 27 such deals.[38] These put the country at the centre of a complex network of commitments to enable data flows with other countries.[39] This means that restrictions on onward transfers of EU data from Singapore to third parties might conflict with the terms of other digital trade agreements concluded by Singapore. Which trade agreement takes precedent in that situation is not clear. Singapore might be forced into a trade dispute with regard to the transfer of EU data to a third country.

The Global Privacy Assembly (GPA), which brings together most data protection regulators, including those in the EU, recently issued a joint resolution on data flows with trust. This authoritative document makes clear that 'onward transfers… should be allowed only if the level of protection… established for the initial transfer are not undermined.'[40] Whatever approach the Commission takes to improving personal data transfers to Singapore, there is a need for clearer guarantees on the status of onward transfers to ensure that the fundamental rights and freedoms of people in Europe are protected.

If such guarantees are not possible, regulators may need to stop certain transfers, but this may be challenged under the terms of the DTA. Many countries, including the United States, have regulatory requirements to keep some data within the country. For example, financial regulators obtained carve- outs in US digital trade agreements, while health information covered by the Health Insurance Portability and Accountability Act (HIPAA 1996) can only be sent abroad if certain standards are met.

The European Data Protection Supervisor (EDPS) has questioned whether the agreement provides enough legal certainty to ensure that certain data is kept in the EU if needed.[41]. Regulators and public bodies in areas such as finance and law enforcement may need to ensure that certain data remains within their reach.

RISK 4 – IT UNDERMINES WORKERS' RIGHTS

The world of work is completely permeated by digital technologies. Digitalisation unavoidably impacts workers because the internet enables the offshoring of many jobs, from call centres and what is generally known as the business process outsourcing (BPO) sector, to the provision of selected professional services. At the same time, developments in AI and other technologies are transforming these jobs with unclear outcomes.[42]

DTA clauses on data and source code may affect particular new categories of work that have been created specifically by these technologies.

Platform workers who depend on digital software for their job allocations and wages are at the forefront of initiatives to improve the governance of digital systems in the workplace. Organisations such as Worker Info Exchange have found that 'employment law does not have the necessary provisions to fully protect workers from the unfair practices stemming from algorithmic management.'[43] Instead they have used various rights under the GDPR. In 2020, Uber drivers litigated in the Netherlands to increase the data shared by the company with workers to allow them to address their workload and wages.

Understanding algorithmic management is a growing concern throughout Europe. Italian delivery couriers obtained an order from the Italian data authority against their employer for failing to provide enough information on their work-related algorithms. The case required an extensive forensic technical evaluation of the mobile phone apps used by the employer to allocate work and measure performance. This was 'black-box testing' without access to the source code, which showed potential privacy violations.[44] However, scaling such painstaking forensic work to a multitude of companies across the EU is not sustainable.

EU Member States such as Spain have passed laws to protect the labour rights of people engaged in distribution and delivery through digital platforms. Better known as the 'Riders' Law', this legal framework improves algorithmic transparency by requiring companies to disclose technical details to workers' representatives.[45]

The EU has recently adopted a Platform Work Directive[46] (PWD) that, among other improvements to labour conditions, establishes clearer rules on data and algorithmic management.[47] These address the limitations of the GDPR created by employment-related carve-outs. The PWD provides for an outright ban on the processing of certain categories of data, including emotional analysis, and improves transparency and explanation rights.[48] Some critics have pointed out that these provisions should extend to all workers.[49]

The PWD details some of the information that must be made available, which includes 'categories of data and the main parameters that such systems take into account and the relative importance of those main parameters in the automated decision-making'. Article 21 of the PWD requires countries to ensure that courts or competent authorities have wide latitude to 'order the digital labour platform to disclose any relevant evidence which lies in its control'. Singapore has recently passed a Platform Workers Act that introduces limited rights and protections but does not contain data-related measures similar to those of the EU Directive.[50]

The ban on requiring access to source code contained in the EUSDTA conflicts with labour protections requiring algorithmic scrutiny. Accessing algorithmic information to address unfair practices in platform work, including potential discrimination or privacy violations, will be made more difficult by the digital trade agreement with Singapore. While the agreement might give government authorities the right to demand certain types of information in the event that they suspect abuse by companies, workers and watchdogs will not have access to the data they produce.

Workers are incrasingly demanding the right to access the data they produce and to participate in data governance. The EUSDTA undermines these requests and instead cements companies' exclusive ownership of the data collected from workers[51].

Even though there are currently no gig platforms operating in Europe from Singapore, given its central role as a base for tech companies, it is realistic to think that this could happen in the future.

RISK 5 – LOSING CONTROL OVER DATA UNDERMINES THE EU'S DIGITAL INDUSTRIALISATION EFFORTS

The EU is scrambling to find ways to be less dependent on external technology from the United States and China, and it is not alone. Countries such as Brazil and India are loudly reclaiming their 'digital sovereignty… to exercise power and control over digital infrastructure, data, services, and protocols'.[52] The EUSDTA will hamper efforts to develop European digital technology by constraining potential industrial strategies.

In order to secure the free flow of data, the agreement with Singapore prohibits governments from demanding that companies localise data and computing facilities within their territories. The EU justifies this requirement on the basis that it avoids additional costs and administrative burdens for European businesses. They argue that requiring companies to store data in the territory where they operate means that they have to build and maintain data storage facilities in multiple places and duplicate the data they use, with a negative impact on their competitiveness. A 2017 US Government survey of businesses found that businesses saw forced localisation as one the main problems for the cross-border delivery of services online[53], particularly in Asia.[54]

However, data is an important part of the development of modern technologies across all sectors, not just digital and tech. The large amount of data generated in the EU represents a huge potential for innovation and competitiveness. Policies for the development of domestic industries and increasing investment in domestic digital infrastructure by non-EU companies may require some digital localisation.

The EU's digital industrial policy is guided by flagship initiatives that include the new Competitiveness Compass, the Digital Compass 2030[55] and the European Industrial Strategy. These frameworks establish ambitious targets for Europe's digital transformation, including doubling the EU's share of global semiconductor production to 20 % by 2030 and ensuring that 75 % of European enterprises adopt cloud computing, artificial intelligence and big data technologies. These targets imply the creation of data centres and other physical infrastructure in Europe that appear at odds with the commitments in the DTA on banning the mandatory localisation of data and computing facilities.

The EUSDTA goes even further, including bans on the mandatory use of standards or specific technologies. It is likely that these measures conflict with industrial policies designed to create a European digital industry and establish strategic autonomy from the main global powers – the United States and China – in critical technological domains.

Initiatives such as the European Chips Act,[56] which aims to strengthen semiconductor manufacturing capabilities within the EU, could be at risk, as could other regulations that support the EU's digital strategy to reduce dependence on non-EU technology providers while fostering European technological capabilities.

A new wave of proposals has put new urgency on these efforts and a new wave of proposals is under way, such as the Eurostack,[57] which go further and include calls for developing not just digital services but an integrated supply that includes minerals, semiconductors and hardware. These proposals may address the need, as MEP Li Andersson has put it, for "a positive (non-dystopian) vision of what digital services and the Internet can look like"[58].As such, the Eurostack is not trying to build a digital wall for Europe. Francesca Bria, one of the leads in the Eurostack project, argued these efforts should look past the EU, "working alongside countries like Brazil, Taiwan, and India"[59] collaborating in open technologies.

The impact on common European data spaces

Common European data spaces are structured frameworks for data sharing within specific sectors across the EU, aiming to build 'the single market for data'.[60] Established under the 2020 European Data Strategy, these spaces create secure environments in which businesses, public bodies and individuals can share data while maintaining control over its use. They focus on key sectors, including health, manufacturing, agriculture, finance, mobility, energy and the European Open Science Cloud.

The data spaces provide technical infrastructure, governance mechanisms and standards for interoperability to enable efficient data exchange between participants.

While not explicitly mandating localisation, the practical implementation of these spaces – with their emphasis on European standards, values and regulatory frameworks – may create de facto data localisation effects. These spaces show the challenges of reconciling commitments to international digital trade openness with efforts to build European digital sovereignty.

Some specific data spaces may require additional restrictions on data transfers – for example, the European Financial Data Space (EFDS) under the recent proposal for a Regulation on Financial Data Access.[61] Similarly, the European Health Data Space would enable EU citizens to control their electronic health data while making it possible for researchers, innovators and policymakers to use such data in a trusted and secure way that preserves privacy.[62] These proposals seem incompatible with the prohibition on data localisation contained in the Singapore DTA.

The EDPS has raised concerns about the potential conflict between these health spaces and the anti-localisation measures contained in the EU Korea digital trade agreement: 'For the avoidance of doubt, the EDPS recommends to expressly clarify in the negotiating directives that the negotiated rules should not prevent the EU or the Member States from adopting, in duly justified cases, measures that would require controllers or processors to store personal data in the EU/EEA" [63]

Although the EDPS's comments relate specifically to the DTA with Korea, they could equally apply to Singapore.

Clashes with the EU's Data Governance Act (DGA) and Data Act

Both the EU's Data Governance Act (DGA)[64] and Data Act[65] promote the creation of a European data economy. One of the key objectives of these pieces of legislation is to achieve greater control over data flows and restrictions on cross-border transfers of sensitive non-personal data.

Non-personal data encompasses all information that cannot be used to identify individuals – such as industrial machine outputs, anonymised datasets and aggregated statistics – and has become critically important as the foundation of digital innovation, economic competitiveness and strategic autonomy in today's data-driven economy.

The objectives of the DGA and Data Act potentially clash with digital trade agreements on account of their fundamental approach to data governance. While the EUSDTA promotes unrestricted cross-border data flows, these EU regulations apply a different philosophy. They establish specific restrictions on transfers of non-personal data outside the EU, require permissions for transferring protected data, and mandate data sharing in certain instances, which could conflict with the provisions on the free flow of data.

Accordingly, the EU's strategic vision for data governance and protection of commercially sensitive information conflicts with the free flow provisions and disclosure prohibitions found in digital trade agreements such as the ESDTA.

RISK 6 – THE ABILITY TO TAX BIG TECH IN EUROPE MAY BE LOST

Digital trade agreements, such as the EUSDTA, could hamper the regulatory autonomy of the EU and Member States with regard to taxation.

There are ongoing international efforts by the OECD to harmonise taxes at the international level, alongside an initiative, supported by most countries, to create a UN tax convention[66], and a number of EU countries have implemented digital service taxes. The United States has launched a major offensive against the OECD's efforts, which they see as 'discriminatory and extraterritorial tax measures'.[67] Tax experts warn that the recent activities within the United States should be a 'wake-up call for Europe' that 'reinforces the need for the European Union to develop a unified and resilient tax strategy.'[68]

There are two key provisions in the agreement that could hamper the efforts to tax international technology companies. The first one is a commitment to banning customs duties on electronic transactions that prevents governments from being able to impose tariffs on digital goods and services. This means that buying a physical DVD or a physical book from abroad may incur payment of a tariff, while purchasing a film or book accessed digitally via Apple, Netflix or Amazon would not.

Up to now tariffs have never been levied on digital services, and there are concerns about the impact on consumers, both financially, as costs would be passed on to them, and in terms of the required surveillance of their habits. Nevertheless, tariffs have become a major policy tool since US President Trump's launch of a global trade war, and countries increasingly see them as legitimate forms of income. A UN report estimated that the lack of tariffs on digital services created a revenue loss of USD 5.1 billion for developing countries in 2017,[69] although this figure has been disputed.[70]

The EUSFTA contains clauses to protect the Union's regulatory autonomy to introduce taxation measures 'based on rational criteria' that can differentiate on the basis of the place of incorporation of a company, but not the nationality of the owner. There are also broad provisions allowing policy measures aimed at preventing tax avoidance or evasion. However, it is not clear whether these exceptions will be enough to prevent tax evasion on the part of digital companies.

3.

DEBUNKING THREE CLAIMS ABOUT THE BENEFITS OF THE DTA WITH SINGAPORE

CLAIM 1 – DIGITAL TRADE AGREEMENTS WILL HELP TO BOOST TRADE IN DIGITAL GOODS AND SERVICES

The European Commission's primary rationale for pursuing and justifying the signing of digital trade agreements, including the one with Singapore, is that digital trade in the EU has grown. It notes that 55 % of total EU trade in services is delivered digitally and that 55 % of EU-Singapore trade occurs digitally too[71]. The EU emphasises that agreements such as the EUSDTA are critical for economic growth.

While the Commission automatically assumes that digital trade agreements will contribute to the growth of trade in digital services, there are no impact assessments to justify how specific measures will have the positive impacts desired.

Facilitating data flows through regulatory alignment may have a positive impact on growth, but a simple causation is not obvious. Through adequacy decisions, the EU already has a free flow of data regime with countries such as Argentina, Uruguay and New Zealand, which goes much further than the DTAs. This is very positive for businesses trading with those countries, but clearly not enough to trigger a boom in services trade. By contrast, China has a challenging environment for data flows from the EU, without clear economic harms. The current understanding from the OECD, which is taking the lead in examining the relationship between data flows and economic growth, is that countries need to find a golden medium between extremes of data autarky and localisation vs unrestricted flows.[72]

The ban on requiring access to source code is a completely distinct case and lacks any economic basis to justify the explicit risks to legislation affecting important objectives of general public interest. This is particularly concerning in the middle of a major dispute over digital regulation with the United States, where the current administration has shown that it will use any means, whether direct or indirect, to exert pressure on its counterparts.

CLAIM 2 – A BAN ON DATA LOCALISATION REQUIREMENTS HELPS SMES

The European Commission has made the case that digital trade agreements are beneficial to small and medium enterprises (SMEs) because they ban costly data localisation requirements, an unnecessary burden for businesses. If true, this would be an important point, as 99 % of European businesses are SMEs, providing jobs to more than 85 million European citizens and residents.[73]

However, the reality is that in the vast majority of cases EU companies are not forced to store their data elsewhere and the EU digital strategy does not require overseas companies to routinely locate their infrastructure in the bloc. In most cases companies from overseas can participate in the EU digital economy providing that there are safeguards in the transfers of data. We expect this to be similar for EU companies operating in Singapore.

In fact, SMEs may actually be negatively impacted by the data flow with trust approach because this places a greater burden on them than other data transfer approaches.

The best data transfer mechanism for EU companies is for the European Commission to make a formal decision of adequacy over a country or jurisdiction. This means that transfers to that jurisdiction can operate in the same way as transfers within the EU because the legal regime is compatible.

If SMEs use other mechanisms, such as private contracts with privacy guarantees, they are legally responsible for ensuring that the laws of the other jurisdictions do not restrict or undermine these guarantees[74]. Adequacy makes the European institutions responsible for this assessment, taking the burden off companies.

Adequacy is much cheaper than any other data transfer tool. A UK study found that if Great Britain had lost its adequacy decision on account of Brexit, the costs of moving to contracts or certifications would have led to a substantial increase in the cost of conducting cross-border business.[75]

The apparent strategic shift towards digital trade agreements prioritises private contracts and the interoperability of divergent regimes over adequacy and regulatory convergence. This will lead to higher costs over time if it becomes the Commission's modus operandi.

The data flows with trust approach promises a shortcut, but offers no new solutions, while distracting from real work towards achieving concrete transfer mechanisms and future adequacy.

CLAIM 3 – DISCLOSURE OF ALGORITHMS WILL LEAD TO THE FORCED TRANSFER OF TRADE SECRETS AND A LOSS OF BUSINESS VALUE.

The Commission and part of the business community argue that if governments are able to compel companies to provide access to source code as a condition for operating in their country, there is a risk that it might get stolen. Such disclosure of digital assets would destroy a company's business value and might be a disincentive to invest abroad.

There is no clear case or rationale for introducing such clauses in agreements with Singapore and Korea, or other countries such as Japan, where the risk of IP theft or data restrictions is negligible. All of the countries with digital trade agreements with the EU have robust IP frameworks and the rule of law.

The provisions on source code reflect outdated concerns, mainly in relation to China, about potential theft of IP from European companies established in Asia with the excuse of regulation.

The main avenue for forcing technology transfers in China is the requirement to form joint ventures to operate in the country. A survey by the EU Chamber of Commerce in China found that '20 percent of the European firms doing business in China had been pressured to transfer technology, typically through joint ventures".[76] This approach is controversial[77] but in principle it may be a legitimate policy under international law, designed to help domestic development. Many countries, including Japan, have implemented similar policies for years.

The current reality is that it is much more likely that the EU will require access to the source code of imported software than the other way around. Chinese AI companies such as DeepSeek make headlines with cutting edge technology that Western tech companies are keen to copy.[78] There are reports that the Commission is looking into the security risks of Chinese connected cars – which nowadays means most models – following a likely ban of such cars in the United States.[79] Indeed, Chinese media now raise concerns that the EU may force Chinese companies to transfer IP on clean technologies in order to qualify for European subsidies for factories.[80]

Discussions on source code disclosure rarely look at the fundamental question of whether it is necessary at all, as candidly admitted in a well-known "Primer for Trade Negotiators" on source code disclosure: *"We did not, however, ask the important question of whether a general prohibition on requiring the transfer of, and access to, source code is the best way to handle the protection of software innovations in trade agreements. Further research is needed to ascertain that this is the best path to take".*[81]

We could even argue that the policy reflex of including these copycat clauses in all DTAs is a missed opportunity for deeper engagement on how to use trade agreements to truly advance digital technology. Innovation researchers have made the case that the main problem for middle-sized economies such as those of the EU countries is not IP theft but the global zero sum accumulation of intangible assets by 'IP-rich countries", mainly the United States and China.[82] This requires more sophisticated mechanisms than source code restrictions.

The aim of a ban on requiring access to source code is not to prevent IP theft but to create a shadow regime of intellectual property (IP) that goes beyond the EU regime[83].

The ban on requring access to source code would extend the protection of trade secrets to potentially restricting legitimate forms of 'reverse engineering', i.e. reconstructing the underlying logic and rewriting the code, and in some cases extracting the source code (a challenging process called decompilation).

EU law specific to software allows some limited forms of reverse engineering for legitimate purposes include enabling interoperability, or fixing problems that the original developer cannot or will not fix[84].

Even under the Trade Secrets Directive (EU Directive 2016/943) reverse engineering is allowed under certain circumstances.

The digital trade clauses could put a ratchet on the EU regime, 'establishing exclusivities over source code and algorithms with only minimal exceptions[85]", and extending these to "algorithms, training materials and data sets, thus creating barriers to accessing information essential for the public interest, including health, safety and policy development.'

The source code clause would be an obstacle to following IP experts' calls for wider reforms of the trade secret regime to introduce clear public interest exceptions, similar to copyright or patents[86], and more flexibility in the EU software regime.[87]

4.

WHY THE EXCEPTIONS IN THE DTA WITH SINGAPORE ARE NOT ENOUGH TO PROTECT PUBLIC POLICY, WORKERS AND CONSUMERS

The common response from the European Commission to the criticisms and questioning of digital trade policies is not to engage on whether the disciplines imposed would be helpful. Instead, the main counterargument is that all the concerns about hampering regulation, industrial development and creating privacy risks are addressed through the exceptions and safeguards in the trade agreements.

The Commission approach is to rely on exceptions that have not been tested in practice. In the history of trade and investment policy, exceptions have proven to be very difficult to invoke in practice. The majority of cases in which countries have tried to rely on exceptions to counter claims at the WTO or at international arbitration tribunals have failed.

The exceptions in the EUSDTA are indeed extensive, although narrow in scope. We find the wholesale incorporation of exceptions in relation to general public policy, security and taxation from the original 2019 FTA. There is also a 'prudential carve-out' to ensure the stability of the financial system. A broad clause on *the right to regulate* lists specific public policy objectives[88], which include privacy and cultural diversity, among others. These provisions complement specific exceptions in relation to restricting data flows and requiring access to source code.

These multi-layered safeguards interact with each other in a complex manner, meaning that any detailed interpretation must look carefully at the entire body of texts and at wider trade law. The expansion of the language on exceptions in the EUSDTA clearly shows that the EU is aware of the risks that some of the clauses can pose to public policy. Despite the number of exceptions included, the implementation of digital trade exceptions is a highly technical and disputed area in which there is no agreement owing to the lack of jurisprudence. There is no evidence to confirm that the exceptions would be sufficient to mitigate the clear risks of some of the clauses included in the treaty.

Furthermore, lawyers have highlighted that the 'material risk' to regulatory flexibility is not limited to legal challenges but includes 'regulatory chill, where policymakers may under-regulate to avoid potential conflicts with trade commitments'[89].

In summary, there is significant uncertainty with regard to relying on exceptions, and unfortunately the situation will only become clearer once a conflict between digital trade and EU policies is litigated and results in dispute mechanisms followed by a ruling. In the meantime, the EU will be gambling its digital future on the vagaries of complex trade laws.

EXCEPTION 1 – ACCESS TO SOURCE CODE

The agreement with Singapore includes specific exceptions to the main rule that prohibits parties from requiring disclosure of source code as a condition for conducting business. In essence:

1) regulatory authorities, law enforcement agencies and courts can still require access to source code 'to ensure compliance with laws that serve legitimate public policy goals'.

2) courts and competition authorities can also require 'proportionate and targeted access to the source code of software' to address violations of competition law or ensure fair competition in digital markets, as long as such access is not 'inconsistent with the Agreement'.

From a government regulatory perspective, these exceptions have several potential flaws that could hinder a government's ability to regulate effectively:

The exceptions are too ambiguous and potentially subject to broad interpretation

- Terms such as 'legitimate public policy objectives' and 'proportionate and targeted access' are subjective and could be interpreted broadly. It is not clear who will determine what constitutes a legitimate objective.
- Companies can challenge a government bodies request as being unjustified or disproportionate.
- the 'proportionate and targeted' qualifiers could make it difficult for competition authorities to conduct comprehensive investigations into digital market dominance.

They are narrow in scope: they do not foresee civil society oversight

- The exceptions primarily focus on government bodies and courts, but make no provisions for non-governmental organisations, trade unions, consumer protection groups or other watchdog organisations to access source code for legitimate scrutiny in the public interest.
- This creates an accountability gap in which software that affects workers' rights, consumer protection, the environment and social equity can operate without independent verification by civil society.
- Without access rights for these watchdog entities, potential harms may go undetected, particularly in areas where government regulation is weak or where regulators have limited technical capacity.
- This imbalance could undermine the important role that civil society plays in the democratic oversight of technological systems and their impacts on vulnerable communities.

There are key risks that are not even contemplated in the exceptions

- The exceptions may not be sufficiently future-proofed to take account of rapidly evolving technologies, leaving governments unable to adapt regulatory approaches for new software paradigms.
- The exceptions may not provide sufficient clarity on the extent to which governments can require source code access for legitimate regulatory purposes, potentially chilling regulatory action due to fear of violating the terms of the agreement.

A comprehensive study on the interaction of AI and trade policy in the closely-related UK context has found that '[d]ifficulties exist at both the "rule" and "exception" level'. It argues that agreement-wide exceptions, chapter-wide exceptions, and article-specific exceptions are narrow in scope and 'may still unduly constrain the development of a robust regime for AI regulation and auditing'.[90]

Given these widespread concerns on the part of experts about the use of exceptions, the generic assurances from the European Commission that there will be no conflict with EU law or regulatory oversight in the future should be backed by full transparency and publication of any internal assessments of how the exceptions are sufficient to overcome the risks.

EXCEPTION 2 – PRIVACY OF PERSONAL DATA AND GDPR COMPLIANCE

The Commission claims that 'the agreement expressly preserves the EU's high level of protection for personal data and privacy'[91]. In 2018, the EU adopted horizontal provisions on cross-border data flows and the protection of personal data and privacy (the 'Horizontal Provisions')[92]. These provisions preserve the high level of protection of data privacy guaranteed by the Charter of Fundamental Rights of the European Union.

The agreement does include a specific exception on personal data protection where countries commit to 'recognise that individuals have a right to privacy and the protection of personal data...'.

At first sight this seems like a solid exception. However, the EDPS, the EU's independent data protection authority, concluded in its opinion of March 2025 that 'the legal wording of the Horizontal Provisions was modified in the Digital Trade Agreement. As a result, the EDPS is concerned that the Digital Trade Agreement, in its current wording, could – contrary to the negotiating directives contained in the Recommendation – affect the EU's personal data protection rules and the possibility for the EU to, in duly justified cases, enact measures that would require controllers or processors to store personal data in the EU/EEA'[93].

There are well-known concerns about the GDPR not being able to survive a legal challenge in a trade arbitration tribunal.[94] The EDPS opinion also noted that Article 6 (on data protection) 'does not state that "[n]othing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards"'. This omission would make it more difficult to defend laws protecting privacy and related to data protection in a WTO dispute.

EXCEPTION 3 – RIGHT TO REGULATE

The European Commission claims that the agreement with Singapore preserves the right to regulate because it has incorporated an article whereby 'The Parties reaffirm their right to regulate within their territories to achieve legitimate policy objectives, such as the protection of public health, social services, public education, safety, environment or public morals, social or consumer protection, privacy and data protection, and the promotion and protection of cultural diversity'.

The right to regulate in the public interest is one of the customary rights of a sovereign state. Reaffirming the right to regulate does not mean that the government cannot be sued for policies that violate disciplines under the agreement, even where these are designed to achieve legitimate policy objectives. The only way to completely safeguard policy space from lawsuits is by excluding certain provisions or the entire digital trade chapter from the agreement's dispute settlement mechanism.

Experts have argued that *'the inclusion of the right to regulate is superfluous.'* [95] *Crucially, they explain that 'each sovereign state has the right to regulate in its public interest… but the right to regulate in WTO [trade] law does not function as an à la carte exception'. WTO jurisprudence explicitly states that the role of trade agreements is precisely to 'discipline the exercise of [countries'] inherent power to regulate by requiring [them] to comply with the obligations that they have assumed'.*

This takes us back to the core question of the implementation of exceptions, which in the EUSDTA follow the basic WTO trade law contours of necessity and proportionality and non-discrimination, but with less stringent criteria. The exceptions include a long list of legitimate objectives with current concerns around online safety, artificial intelligence, disinformation and social cohesion. This may help with the interpretation in the event of a dispute, but it will not prevent the dispute.

EXCEPTION 4 – GENERAL EXCEPTION

The agreement with Singapore includes a so-called general exception clause. This follows the language of the WTO general exceptions (Articles XX of GATT and Article XIV of GATS).

As the general exceptions clause for digital trade measures has never been invoked there is no jurisprudence on how effective it would be. However, the experience from the WTO shows that it is almost impossible to apply. Of 48 cases in which a government attempted to invoke the general exception in a WTO tribunal, only two were successful.[96]

5.

CONCLUSIONS

In conclusion, the analysis presented in this report paints a concerning picture of the EU-Singapore Digital Trade Agreement (EUSDTA). Rather than giving digital trade a straightforward boost, the agreement will pose **significant risks** to the EU's future. These include restricting the EU's policy space to regulate the digital sector, undermining existing EU digital regulations such as the DSA, DMA and AI Act, jeopardising the protection of European personal data flowing to Singapore, undermining workers' rights, hindering the EU's digital industrialisation efforts on account of a loss of control over data, and complicating the taxation of Big Tech companies.

The European Commission's claims about the benefits of the EUSDTA are not substantiated by evidence. It is likely that digital trade growth is driven by technological advancements rather than by such agreements, that a ban on requiring data localisation might negatively impact SMEs, and that concerns about the disclosure of algorithms leading to the theft of trade secrets are overstated, especially with partners such as Singapore.

Crucially, the **exceptions included in the DTA are insufficient** to adequately protect public policy, workers and consumers. The ambiguity and narrow scope of the exceptions relating to source code access, data protection and the right to regulate are major weaknesses. In trade law history, invoking exceptions has in practice proven to be very difficult. The loopholes and language of the exceptions in the DTA with Singapore are insufficiently robust to allow the assumption that their application will be any more effective.

The EU is **taking a significant gamble** with its digital future by relying on complex and untested trade law exceptions to mitigate the substantial risks associated with the EUSDTA.

An in-depth assessment of the agreement's clauses and exceptions suggests that the potential downsides of the EUSDTA for the EU's regulatory autonomy, data protection standards, workers' rights and digital industrialisation ambitions outweigh the claimed benefits, and that the effectiveness of the built-in safeguards remains highly questionable.

6.

RECOMMENDATIONS FOR A NEW EU DIGITAL TRADE APPROACH

1. MODERNISE THE EU DIGITAL TRADE FRAMEWORK

Stop reproducing the text of outdated trade agreements originating from the United States and Asia-Pacific and develop a comprehensive digital trade approach that maintains flexibility for public interest regulation while addressing rapid technological advancement. This framework should:

- establish clear principles that balance innovation with regulatory sovereignty
- include regular review mechanisms to adapt to technological developments
- prioritise democratic oversight of digital trade policies over fragmented engagement with stakeholders.
- prioritise specific facilitation mechanisms with demonstrable effects on trade, such as the digitisation of documents.

2. ELIMINATE SOURCE CODE RESTRICTIONS

Remove all provisions restricting access to source code in trade agreements. Rather than creating complex exception regimes, implement:

- complete elimination of clauses limiting source code access
- affirmative language supporting transparency and auditability
- recognition of algorithmic accountability as a core regulatory principle

3. STRENGTHEN DATA PROTECTION THROUGH HORIZONTAL CLAUSES

Implement horizontal clauses that ensure consistent data protection standards across all digital trade provisions:

- Establish data protection as a fundamental right rather than a trade barrier
- Ensure that these horizontal protections cannot be undermined by sectoral provisions
- Develop enforcement mechanisms for these protections

4. PRIORITISE ADEQUACY-BASED DATA TRANSFER MECHANISMS

Replace 'free flow of data' commitments with concrete transfer mechanisms based on adequacy decisions:

- Develop paths for mutual recognition frameworks for data protection regimes
- Create pathways for regulatory convergence that respect EU data protection standards
- Establish monitoring systems to evaluate ongoing compliance with adequacy requirements

5. ENSURE CAPACITY FOR STRATEGIC DIGITAL LOCALISATION CARVE-OUTS

Following EDPS recommendations, create specific carve-outs for digital infrastructure located within the EU:

- Define clear parameters for European data spaces
- Identify strategic sectors requiring data localisation or domestic computing facilities
- Establish governance frameworks for these protected data environments

6. COMMISSION AN AUTHORITATIVE DIGITAL TRADE POLICY REVIEW

Initiate a comprehensive expert assessment to resolve tensions between digital trade commitments and the regulatory autonomy of the digital economy:

- Analyse conflicts between existing agreements and EU regulatory frameworks
- Evaluate the effectiveness of current exception mechanisms
- Provide evidence-based recommendations for policy coherence
- Analyse the impact of digital trade agreements

7. PAUSE DIGITAL TRADE NEGOTIATIONS

- Implement a moratorium on new digital trade agreements pending a policy review:
- Pause ongoing negotiations and the signing of digital trade agreements
- Establish clear criteria for resuming negotiations based on review outcomes
- Use this period to develop stakeholder consultation mechanisms.

ANNEX - TABLE COMPARING KEY DIGITAL TRADE CLAUSES IN FTAS

	EU-NZ FTA[a]	EU-Chile FTA[b]	EU-Japan[c]	EU-Singapore[d]	EU-South Korea[e]
Free flow of data and data localisation	*Article 12.4* **Cross-border data flows**	*Article 19.4* **Cross-border data flows: prohibition of data localisation**	*Article 8.81* **Cross-border transfer of information by electronic means**	*Article* 5 **Cross-border data flows**	*Article 5* **Cross-border data flows**
	1. The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy and recognise that each Party may have its own regulatory requirements in this regard.	The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy.	1. The Parties are committed to ensuring the cross-border transfer of information by electronic means where this activity is for the conduct of the business of a covered person.	1. The Parties are committed to ensuring the cross-border transfer of data by electronic means where this activity is for the conduct of the business of a covered person.	1. The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy and recognise that each Party may have its own regulatory requirements in this regard.
	2. To that end, a Party shall not restrict cross-border data flows taking place between the Parties in the context of activity that is within the scope of this Chapter, by:	To that end, cross-border data flows shall not be restricted between the Parties by:	2. To that end, a Party shall not adopt or maintain measures which prohibit or restrict the cross-border transfer of information set out in paragraph 1 by:	2. To that end, a Party shall not adopt or maintain measures which prohibit or restrict the cross-border transfer of data set out in paragraph 1 by:	2. To that end, a Party shall not adopt or maintain measures which prohibit or restrict cross-border transfer of data between the Parties by:
	(a) requiring the use of computing facilities or network elements in its territory for data processing, including by requiring the use of computing facilities or network elements that are certified or approved in the territory of the Party;	a) requiring the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of the Party;	(a) requiring the use of computing facilities or network elements in the territory of the Party for information processing, including by requiring the use of computing facilities or network elements that are certified or approved in the territory of the Party;	a. requiring the use of computing facilities or network elements in the Party's territory for processing of data, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of the Party;	a. requiring the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of the Party;
	(b) requiring the localisation of data in its territory;	b) requiring the localisation of data in the Party's territory for storage or processing;	(b) requiring the localisation of information in the territory of the Party for storage or processing;	b. requiring the localisation of data in the Party's territory for storage or processing;	b. requiring the localisation of data in the Party's territory for storage or processing;
	(c) prohibiting storage or processing of data in the territory of the other Party; or	c) prohibiting storage or processing in the territory of the other Party;	(c) prohibiting storage or processing of information in the territory of the other Party;	c. prohibiting storage or processing of data in the territory of the other Party;	c. prohibiting storage or processing in the territory of the other Party;
	(d) making the cross-border transfer of data contingent upon the use of computing facilities or network elements in its territory or upon localisation requirements in its territory.	d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Party's territory or upon localisation requirements in the Party's territory.	(d) making the cross-border transfer of information contingent upon use of computing facilities or network elements in the territory of the Party or upon localisation requirements in the territory of the Party;	d. making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Party's territory or upon localisation requirements in the Party's territory; or	d. making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Party's territory or upon localisation requirements in the Party's territory;
			(e) prohibiting the transfer of information into the territory of the Party; or	e. prohibiting the transfer of data into the territory of the Party.	e. prohibiting the transfer of data into the territory of the Party; or
			(f) requiring the approval of the Party prior to the transfer of information to the territory of the other Party.		f. requiring the approval of the Party prior to the transfer of data to the territory of the other Party.
	Exceptions see below	*Exceptions see below*	*Exceptions see below*	*Exceptions see below*	*Exceptions see below*

	EU-NZ FTA[a]	EU-Chile FTA[b]	EU-Japan[c]	EU-Singapore[d]	EU-South Korea[e]
Free flow of data and data localisation	*Article 12.11 -* **Transfer of or access to source code**	*Article 19.12 -* **Prohibition of mandatory transfer of or access to source code**	**No article on source code**	*Article 11 -* **Source code**	*Article 11 –* **Source code**
	1. The Parties recognise the increasing social and economic importance of the use of digital technologies, and the importance of the safe and responsible development and use of such technologies, including in respect of source code of software to foster public trust.	1. No Party may require the transfer of, or access to, source code of software owned by a juridical or natural person of the other Party.		1. Neither Party shall require the transfer of, or access to, the source code of software owned by a natural or juridical person of the other Party as a condition for the import, export, distribution, sale or use of such software, or of products containing such software, in or from its territory.	1. Neither Party shall require the transfer of, or access to, source code of software owned by a natural or juridical person of the other Party, as a condition for the import, export, distribution, sale, or use of that software, or of products containing that software, in or from its territory.
	2. A Party shall not require the transfer of, or access to, the source code of software owned by a person of the other Party as a condition for the import, export, distribution, sale or use of such software, or of products containing such software, in or from its territory.				
	Exceptions see below	*Exceptions see below*	*Exceptions see below*	*Exceptions see below*	*Exceptions see below*
Customs duties on electronic transmissions	*ARTICLE 12.6 -* **Customs duties on electronic transmissions**	*Article 19.6 -* **Customs duties on electronic transmissions**		*ARTICLE 7 –* **Customs duties**	*ARTICLE 7 -* **Customs duties on electronic transmissions**
	1. A Party shall not impose customs duties on electronic transmissions between a person of one Party and a person of the other Party.	1. No Party shall impose customs duties on electronic transmissions between a person of one Party and a person of the other Party.		The Parties shall not impose customs duties on electronic transmissions.	1. Neither Party shall impose customs duties on electronic transmissions.
	2. For greater certainty, paragraph 1 shall not preclude a Party from imposing internal taxes, fees or other charges on electronic transmissions, provided that such taxes, fees or charges are imposed in a manner consistent with this Agreement.	2. Paragraph 1 does not apply to telecommunications services, broadcasting services, gambling services, legal representation services, nor to services of notaries or equivalent professions to the extent that they involve a direct and specific connection with the exercise of public authority.			2. For greater certainty, paragraph 1 does not preclude a Party from imposing internal taxes, fees, or other charges on electronic transmissions in a manner not inconsistent with this Agreement.

	EU-NZ FTA[a]	EU-Chile FTA[b]	EU-Japan[c]	EU-Singapore[d]	EU-South Korea[e]
No prior authorisation	*Article 12.7 -* **No prior authorisation**	*Article 19.7 -* **No prior authorisation**		*Article 8 –* **No prior authorisation**	*Article 8 –* **No prior authorisation**
	1. Each Party shall endeavour not to impose prior authorisation or any other requirement having an equivalent effect on the supply of services by electronic means.	1. A Party shall not require prior authorisation solely on the ground that a service is provided online1 or adopt or maintain any other requirement having equivalent effect.		1. A Party shall not require prior authorisation solely on the ground that a service is provided online, or adopt or maintain any other requirement having an equivalent effect.	A Party shall endeavour not to require prior authorisation solely on the ground that a service is provided online, or adopt or maintain any other requirement having an equivalent effect.
	2. Paragraph 1 shall be without prejudice to authorisation schemes that are not specifically and exclusively targeted at services provided by electronic means, and to rules in the field of telecommunications.			2. Paragraph 1 does not apply to telecommunications services, broadcasting services, gambling services, or legal representation services, nor to services of notaries or equivalent professions to the extent that they involve a direct and specific connection with the exercise of public authority.	

EXCEPTIONS					
Protection of personal data and privacy	*Article 12.5 -* **Protection of personal data and privacy**	*Article 19.5 -* **Protection of personal data and privacy**	*Article 8.82 -* **Protection of Personal Data**	*Article 6 -* **Personal data protection**	*Article 6 -* **Protection of personal data and privacy**
	1. Each Party recognises that the protection of personal data and privacy is a fundamental right and that high standards in this regard contribute to enhancing consumer confidence and trust in digital trade.	1. Each Party recognises that the protection of personal data and privacy is a fundamental right and that high standards in this regard contribute to trust in the digital economy and to the development of trade.	1. The Parties recognise that individuals have a right to the protection of their personal data and privacy as provided for by the laws and regulations of each Party and that high standards in this regard contribute to trust in the digital economy and to the development of trade. Each Party recognises the right of the other Party to determine the appropriate level of the protection of personal data and privacy, to be provided for by their respective measures.	1. Parties recognise that individuals have a right to privacy and the protection of personal data and that high and enforceable standards in this regard contribute to trust in the digital economy and to the development of trade.	1. Each Party recognises that individuals have a right to the protection of personal data and privacy and that high standards in this regard contribute to enhancing consumer confidence in the digital economy and to the development of trade.

	EU-NZ FTA[a]	EU-Chile FTA[b]	EU-Japan[c]	EU-Singapore[d]	EU-South Korea[e]
Protection of personal data and privacy	2. Each Party may adopt or maintain measures it deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data. Nothing in this Agreement shall affect the protection of personal data and privacy afforded by the Parties' respective measures.	2. Each Party may adopt and maintain the measures it deems appropriate to ensure the protection of personal data and privacy, including the adoption and application of rules for the cross-border transfer of personal data. Nothing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective measures.	2. Each Party shall endeavour to adopt measures that protect individuals, without discrimination based on grounds such as nationality or residence, from personal data protection violations occurring within its jurisdiction."	2. Each Party shall adopt or maintain a legal framework that provides for the protection of the personal data of individuals.	2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal data of individuals engaged in digital trade. In the development of its legal framework for the protection of personal data, each Party should take into account principles and guidelines of relevant international bodies with respect to core principles such as lawfulness, data quality, purpose specification, collection and use limitation, limited data retention, data security, transparency, accountability, enforceable rights of individuals such as access, rectification, deletion, independent oversight and effective redress.
	3. Each Party shall inform the other Party about any measures referred to in paragraph 2 that it adopts or maintains.		3. Each Party shall adopt or maintain a legal framework that provides for the protection of personal data related to electronic commerce. In the development of its legal framework for the protection of personal data and privacy, each Party should take into account the principles and guidelines of relevant international bodies. The Parties also recognise that high standards of privacy and data protection as regards government access to privately held data, such as those outlined in the OECD Principles for Government Access to Personal Data held by Private Sector Entities, contribute to trust in the digital economy.	3. In the development of its legal framework for the protection of personal data, each Party should take into account principles and guidelines developed by relevant international bodies or organisations, such as the principles referred to in the Joint Declaration on privacy and the protection of personal data, and the OECD Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data.	3. Each Party shall ensure that its legal framework under paragraph 2 provides non-discriminatory protection of personal data for individuals.

	EU-NZ FTA[a]	EU-Chile FTA[b]	EU-Japan[c]	EU-Singapore[d]	EU-South Korea[e]
Protection of personal data and privacy	4. Each Party shall publish information on the protection of personal data and privacy that it provides to users of digital trade, including:			4. Each Party shall ensure that its legal framework under paragraph 2 provides non-discriminatory protection of personal data for natural persons.	4. Nothing in this Agreement shall prevent a Party from adopting or maintaining measures on the protection on personal data and privacy, including with respect to cross-border data transfers provided that the law of the Party provides for instruments enabling transfers under conditions of general application for the protection of the data transferred.
	(a) how individuals can pursue a remedy for a breach of protection of personal data or privacy arising from digital trade; and	3. For greater certainty, the Investment Court System does not apply to the provisions in Articles 19.4 and 19.5.			5. Each Party shall inform the other Party about any safeguard it adopts or maintains according to paragraph 4.
	(b) guidance and other information regarding compliance of businesses with applicable legal requirements protecting personal data and privacy.		4. Each Party shall publish information on the protection of personal data and privacy it provides to users of electronic commerce, including:	5. Each Party shall publish information on the personal data protections it provides to individuals, including guidance on how:	6. Each Party shall publish information on the protection of personal data and privacy it provides to individuals engaged in digital trade, including guidance on how:
			(a) how individuals can pursue remedies for a breach of the protection of personal data or privacy arising from digital trade; and	(a) individuals can pursue remedies; and,	a. individuals can pursue remedies; and
			(b) guidance and other information regarding compliance of businesses with applicable legal requirements for the protection of personal data and privacy."	(b) enterprises can comply with legal requirements.	b. businesses can comply with legal requirements.
				6. Each Party shall encourage transparency by enterprises in their territory with regard to their policies and procedures related to the protection of personal data.	7. Parties shall endeavour to exchange information and share experiences on the use of mechanisms for the transfer of personal data, as appropriate.

	EU-NZ FTA[a]	EU-Chile FTA[b]	EU-Japan[c]	EU-Singapore[d]	EU-South Korea[e]
Protection of personal data and privacy				7. Recognising that Parties may take different legal approaches to protecting personal data, they should explore ways to increase convergence between these different regimes, including to facilitate cross-border data flows. This may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, broader international frameworks, or joint guidance on the utilisation of common cross-border data transfer mechanisms.	8. For the purposes of this Agreement, 'personal data' means any information relating to an identified or identifiable natural person.
Exceptions to data flows article	*Article 12.4* ***Cross-border data flows***	No exceptions	*Article* 8.81 ***Cross-border transfer of information by electronic mean***s	*Article* 5 - ***Cross-border data flows***	*Article* 5 – ***Cross-border data flows***
	3. For greater certainty, the Parties understand that nothing in this Article prevents the Parties from adopting or maintaining measures in accordance with Article 25.1 (General Exceptions) to achieve the public policy objectives referred to therein, which, for the purposes of this Article, shall be interpreted, where relevant, in a manner that takes into account the evolutionary nature of the digital technologies. The preceding sentence does not affect the application of other exceptions in this Agreement to this Article.		3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraphs 1 and 2 to achieve a legitimate public policy objective, provided that the measure:	4. Nothing in this Article shall prevent a Party from adopting or maintaining a measure inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:	3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective provided that the measure:

	EU-NZ FTA[a]	EU-Chile FTA[b]	EU-Japan[c]	EU-Singapore[d]	EU-South Korea[e]
	4. The Parties shall keep the implementation of this Article under review and assess its functioning within three years after the date of entry into force of this Agreement unless the Parties agree otherwise. A Party may also at any time propose to the other Party to review this Article. Such request shall be accorded sympathetic consideration.		(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade; and	a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and	a. is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
	5. In the context of the review referred to in paragraph 4, and following the release of the Waitangi Tribunal's Report Wai 2522 dated 19 November 2021, New Zealand:		(b) does not impose restrictions on transfers of information that are greater than necessary to achieve the objective."	b) does not impose restrictions on transfers of information greater than are necessary to achieve the objective.	b. does not impose restrictions on transfers of information or the use or location of computing facilities greater than are necessary to achieve the objective.
	(a) reaffirms its continued ability to support and promote Māori interests under this Agreement; and		4. Nothing in this Article shall prevent a Party from adopting or maintaining measures on the protection of personal data and privacy, including with respect to cross-border transfers of information, provided that the law of the Party provides for instruments enabling transfers under conditions of general application for the protection of the information transferred.		4. This Article applies to the cross-border transfer of financial data by a financial service supplier where processing of that data is required in the ordinary course of business of such financial service supplier. Paragraphs 2(a) to (d) shall not apply to the provisions laid down in Article 11(1), and Article 14-2, paragraph 7, of the Regulation on Supervision of Electronic Financial Transactions (Korea Financial Services Commission Notice No.2025-4, February 5, 2025) implementing the Electronic Financial Transactions Act, (Law No.19734, September 14, 2023).

	EU-NZ FTA[a]	EU-Chile FTA[b]	EU-Japan[c]	EU-Singapore[d]	EU-South Korea[e]
	(b) affirms its intention to engage Māori to ensure the review referred to in paragraph 4 takes account of the continued need for New Zealand to support Māori to exercise their rights and interests, and meet its responsibilities under te Tiriti o Waitangi/the Treaty of Waitangi and its principles.		5. This Article does not apply to cross-border transfer of information held or processed by or on behalf of a Party.		5. For greater certainty, paragraphs 3 and 4 do not affect the interpretation of other exceptions in this Agreement and their application to this Article, and the right of a Party to invoke any of them.
					6. The Parties shall keep the implementation of this provision under review and assess its functioning within three years of the entry into force of this Agreement. A Party may at any time propose to the other Party to review the list of restrictions listed in the preceding paragraph. Such request shall be accorded sympathetic consideration.
Exceptions to source code article	*Article 12.11* ***Transfer of or access to source code***	*Article 19.12* ***Prohibition of mandatory transfer of or access to source code***	*Not inclued*	*Article 11* ***Source code***	*Article 11 –* ***Source code***
	3. For greater certainty, paragraph 2:	2. For greater certainty:		2. For greater certainty:	2. For greater certainty:
	(a) does not apply to the voluntary transfer of, or granting of access to, source code of software on a commercial basis by a person of the other Party, for example in the context of a public procurement transaction or a freely negotiated contract; and	a) the general exception, security exception and prudential carve-out can apply to measures of a Party adopted or maintained in the context of a certification procedure;		a. Article 19 (General exceptions), Article 20 (Security exceptions) and Article 18 (Prudential carve-out) may apply to measures of a Party adopted or maintained in the context of a certification procedure;	a) Article 28 [General exceptions], Article 29 [Security exceptions] and Article 27 [Prudential carve-out] may apply to measures of a Party adopted or maintained in the context of a certification procedure;
	(b) does not affect the right of regulatory, administrative, law enforcement or judicial bodies of a Party to require the modification of source code of software to comply with its laws and regulations that are not inconsistent with this Agreement.	b) paragraph 1 does not apply to the voluntary transfer of or granting of access to source code on a commercial basis by a person of the other Party, for instance in the context of a public procurement transaction or a freely negotiated contract;		b. paragraph 1 does not apply to the voluntary transfer of, or granting of access to, source code of software by a natural or juridical person of the other Party on a commercial basis, such as in the context of a public procurement transaction or other freely negotiated contracts, or under open source licenses, such as in the context of open source; and	b) paragraph 1 does not apply to the voluntary transfer of or granting of access to source code on a commercial basis by a natural or juridical person of the other Party, for instance in the context of a public procurement transaction or a freely negotiated contract; and

	EU-NZ FTA[a]	EU-Chile FTA[b]	EU-Japan[c]	EU-Singapore[d]	EU-South Korea[e]
Exceptions to source code article		c) nothing in paragraph 1 prevents a person of a Party from licencing its software on a free and open source basis.		c. paragraph 1 does not affect the right of regulatory, law enforcement or judicial bodies of a Party to require the modification of source code of software to comply with its laws or regulations that are not inconsistent with the Agreement.	c) paragraph 1 does not affect the right of regulatory, law enforcement or judicial bodies of a Party to require the modification of source code of software to comply with its laws or regulations that are not inconsistent with the Agreement.
	4. Nothing in this Article shall:	3. Nothing in this Article shall affect:		3. Nothing in this Article shall affect:	3. Nothing in this Article shall affect:
	(a) affect the right of regulatory authorities, law enforcement, judicial or conformity assessment bodies of a Party to access source code of software, either prior to or following import, export, distribution, sale or use, for investigation, inspection or examination, enforcement action or judicial proceeding purposes, to determine compliance with its laws and regulations, including those relating to non-discrimination and the prevention of bias, subject to safeguards against unauthorised disclosure;	a) requirements by a court, administrative tribunal or, by a competition authority to remedy a violation of competition laws;		a. the right of regulatory authorities, law enforcement, judicial or conformity assessment bodies of a Party to require the transfer of, or access to, source code of software, either prior to or following import, export, distribution, sale or use of such software, for investigation, inspection or examination, enforcement action or judicial proceeding purposes, to secure compliance with its laws or regulations pursuing legitimate public policy objectives subject to safeguards against unauthorised disclosure;	a) the right of regulatory authorities, law enforcement, judicial or conformity assessment bodies12 of a Party to require the transfer of, or access to, source code of software, either prior to or following import, export, distribution, sale or use of such software, for investigation, inspection or examination, enforcement action or judicial proceeding purposes, to secure compliance with its laws and regulations pursuing legitimate public policy objectives13, subject to safeguards against unauthorised disclosure;
	(b) affect requirements by a competition authority or other relevant body of a Party to remedy a violation of competition law;	b) protection and enforcement of intellectual property rights; and		b. the requirements by a court, administrative tribunal, competition authority, or other relevant body of a Party to remedy a violation of competition law, or requirements pursuant to a Party's laws or regulations that are not inconsistent with the Agreement to provide proportionate and targeted access to the source code of software that is necessary to address barriers to entry in digital markets to ensure these markets remain competitive, fair, open and transparent;	b) the requirements by a court, administrative tribunal, competition authority, or other relevant body of a Party to remedy a violation of competition law, or requirements pursuant to a Party's laws or regulations that are not inconsistent with the Agreement to provide proportionate and targeted access to the source code of software that is necessary to address barriers to entry in digital markets to ensure these markets remain competitive, fair, open and transparent;

	EU-NZ FTA[a]	EU-Chile FTA[b]	EU-Japan[c]	EU-Singapore[d]	EU-South Korea[e]
	(c) affect the protection and enforcement of intellectual property rights; or	c) the right of a Party to take measures in accordance with Article 21.3 [security and general exceptions of the Public Procurement Title].		c. the protection and enforcement of intellectual property rights; or	c) the protection and enforcement of intellectual property rights; and
	(d) affect the right of a Party to take measures in accordance with point (a) of Article 14.1(2) (Incorporation of certain provisions of the GPA) under which Article III of the GPA is incorporated into and made part of this Agreement, mutatis mutandis.			d. the right of a Party to take measures in accordance with Article 9.3 (Security and General Exceptions) of the Chapter on Government Procurement of the Free Trade Agreement, which shall apply mutatis mutandis to this Article.	d) the right of a Party to take measures in accordance with Article III [Security and General Exceptions] of the WTO Agreement on Government Procurement.

[a] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202400866#page=262
[b] https://circabc.europa.eu/rest/download/8a25254a-68c0-43e2-8676-f725e69e4696?
[c] https://circabc.europa.eu/ui/group/09242a36-a438-40fd-a7af-fe32e36cbd0e/library/f9c7b4f0-ea0f-467a-bb9e-208013b07312/details
[d] https://circabc.europa.eu/ui/group/09242a36-a438-40fd-a7af-fe32e36cbd0e/library/66ccfa9f-e239-4893-8e12-64f8ff1d1221/details
[e] https://circabc.europa.eu/ui/group/09242a36-a438-40fd-a7af-fe32e36cbd0e/library/1bddb97a-c02e-41e6-95d1-6e41029c880f/details

ENDNOTES

1 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22019A1114%2801%29&qid=1752843208092
2 https://policy.trade.ec.europa.eu/help-exporters-and-importers/accessing-markets/goods-and-services/digital-trade_en
3 https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5378
4 https://ec.europa.eu/commission/presscorner/detail/en/ip_25_732
5 https://www.eeas.europa.eu/sites/default/files/jointcommunication_2021_24_1_en.pdf
6 https://www.mfa.gov.sg/SINGAPORES-FOREIGN-POLICY/Countries-and-Regions/Europe
7 https://eurocham.org.sg/member-directory/
8 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22019A1114(01)&from=EN#page=28
9 https://www.straitstimes.com/world/united-states/go-west-more-singapore-firms-setting-up-shop-in-the-us
10 https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals#:~:text=In%20the%20EU%2C%20the%20share,or%20goods%20online%20in%202024
11 https://www.digitaltrade4.eu/study-on-the-potential-impacts-of-a-future-eu-singapore-digital-trade-agreement/
12 https://ec.europa.eu/newsroom/just/items/627665
13 https://www.edps.europa.eu/data-protection/our-work/publications/opinions/2025-03-21-edps-opinion-42025-proposals-council-decisions-signing-and-conclusion-behalf-union-digital-trade-agreement-between-european-union-and_en
14 https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/october/ustr-statement-wto-e-commerce-negotiations
15 rion, Kristina, AI Regulation in the European Union and Trade Law: How Can Accountability of AI and a High Level of Consumer Protection Prevail over a Trade Discipline on Source Code? (January 26, 2021). Available at SSRN: https://ssrn.com/abstract=3786567 or http://dx.doi.org/10.2139/ssrn.3786567
16 https://publications.parliament.uk/pa/ld5901/ldselect/ldintagr/52/5207.htm#_idTextAnchor039
17 https://opensource.org/ai/open-source-ai-definition
18 Borghi, Maurizio and White, Benjamin, Data Extractivism and Public Access to Algorithms (January 1, 2023). Law, Regulation and Governance in the Information Society: Informational Rights and Informational Wrongs, pp 105-125, 2023, DOI: 10.4324/9781003242987-7, Available at SSRN: https://ssrn.com/abstract=4771780
19 1. De Gregorio G. Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society. Cambridge University Press; 2022. Available at https://www.cambridge.org/core/services/aop-cambridge-core/content/view/A3F61C6368D17D953457234B8A59C502/9781316512777AR.pdf/Digital_Constitutionalism_in_Europe.pdf?event-type=FTLA
20 Jones, Emily and Collins, Philippa and Grosse Ruse-Khan, Henning and Sanchez-Graells, Albert and Irion, Kristina and Dorobantu, Cosmina and Kilic, Burcu and Onitiu, Daria, AI Governance and the Future of Digital Trade Policy (October 09, 2024). University of Oxford Blavatnik School of Government Policy Brief, October 2024, Available at SSRN: https://ssrn.com/abstract=4987769 or http://dx.doi.org/10.2139/ssrn.4987769
21 https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/singapore/eu-singapore-agreements/agreements-explained_en
22 https://knowledge.csc.gov.sg/ai-in-the-public-service-here-for-good/
23 https://www.edb.gov.sg/en/business-insights/insights/how-singapore-can-serve-businesses-as-a-hub-for-ai-innovation-and-growth.html
24 https://www.digitaleducationcouncil.com/post/from-risk-to-opportunity-rethinking-ai-regulation-in-higher-education
25 https://iapp.org/resources/article/global-ai-governance-singapore/ and https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-singapore
26 https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2025/singapore-ai-safety-initiatives-global-ai-summit-france
27 https://www.politico.eu/wp-content/uploads/2018/02/Data-flow-provisions-POLITICO.pdf
28 https://www.mofa.go.jp/ecm/ec/page4e_000973.html
29 https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html
30 http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20_Flows_2020.pdf
31 https://freedomhouse.org/country/singapore
32 https://www.imda.gov.sg/-/media/imda/files/infocomm-media-landscape/research-and-statistics/sgde-report/singapore-digital-economy-report-2024.pdf
33 https://eprints.lse.ac.uk/123885/1/Southeast_Asia_Working_Paper_11.pdf
34 https://www.eeas.europa.eu/sites/default/files/documents/2024/Study%20on%20the%20potential%20impacts%20of%20a%20future%20EU-Singapore%20Digital%20Trade%20Agreement.pdf
35 https://jia.sipa.columbia.edu/content/smart-city-small-state-singapores-ambitions-contradictions-digital-transnational-connectivity
36 https://www.csis.org/analysis/cloud-computing-southeast-asia-and-digital-competition-china
37 https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1896&context=njilb
38 Mira Burri, Maria Vasquez Callo-Müller and Kholofelo Kugler, TAPED: Trade Agreement Provisions on Electronic Commerce and Data, available at: https://unilu.ch/taped Retrieved 30 January 2025
39 For example, Singapore is part of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), and also pioneered the Digital Economy Partnership Agreement (DEPA) with Chile and New Zealand. The agreement includes modules such as "data issues" or "dispute settlement.[1]" https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa As members of CPTPP, the content aligns with the 2020 Singapore Australia Digital Economy Agreement (SADEA) calls for interoperability of data protection regimes. [see Aguerre, C., Campbell-Verduyn, M., & Scholte, J.A. (Eds.). (2024). Global Digital Data Governance: Polycentric Perspectives (1st ed.). Routledge. https://doi.org/10.4324/9781003388418]
40 https://globalprivacyassembly.org/wp-content/uploads/2024/11/Resolution-Data-Free-Flow-with-Trust-and-an-effective-regulation-of-global-data-flows.pdf
41 https://www.edps.europa.eu/system/files/2025-03/25_03_21_opinion_digital_trade_agreement_eu_singapore_en.pdf
42 https://restofworld.org/2025/code-ai-filipino-tech-workers/
43 https://5b88ae42-7f11-4060-85ff-4724bbfed648.usrfiles.com/ugd/5b88ae_8d720d54443543e2a928267d354acd90.pdf
44 https://www.etui.org/sites/default/files/2023-10/Exercising%20workers%20rights%20in%20algorithmic%20management%20systems_Lessons%20learned%20from%20the%20Glovo-Foodinho%20digital%20labour%20platform%20case_2023.pdf
45 https://www.etui.org/sites/default/files/2024-03/Artificial%20intelligence%2C%20labour%20and%20society_2024.pdf
46 https://data.consilium.europa.eu/doc/document/PE-89-2024-INIT/en/pdf
47 https://www.etui.org/publications/eu-platform-work-directive
48 https://www.etui.org/publications/eu-platform-work-directive
49 https://www.europeum.org/wp-content/uploads/silke-merged-final-2.pdf
50 https://www.mom.gov.sg/employment-practices/platform-workers-act/what-it-covers

[51] https://www.etuc.org/en/document/etuc-position-eu-digital-trade-agreements-3rd-countries
[52] https://cyberbrics.info/wp-content/uploads/2024/05/DIGITAL_SOVEREINGTY_IN_BRICS_COUNTRIES_JiangEdits_Jan19-2-2.pdf
[53] https://www.usitc.gov/publications/332/pub4682.pdf
[54] https://www.csis.org/analysis/cloud-computing-southeast-asia-and-digital-competition-china
[55] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en
[56] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en
[57] https://www.euro-stack.info/
[58] https://www.ianbrown.tech/2024/09/26/2061
[59] https://ainowinstitute.org/publication/x-european-digital-independence-building-the-eurostack
[60] https://digital-strategy.ec.europa.eu/en/policies/data-spaces
[61] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0360
[62] https://ec.europa.eu/newsroom/dae/redirection/document/101623
[63] https://www.edps.europa.eu/data-protection/our-work/publications/opinions/2023-05-15-edps-opinion-182023-recommendation-council-authorising-opening-negotiations-digital-trade-disciplines-republic-korea-and-singapore_en
[64] https://digital-strategy.ec.europa.eu/en/policies/data-governance-act
[65] https://digital-strategy.ec.europa.eu/en/policies/data-act
[66] https://taxjustice.net/2025/02/05/trumps-walkout-fumble-is-a-golden-window-to-push-ahead-with-a-un-tax-convention/
[67] https://www.whitehouse.gov/presidential-actions/2025/01/the-organization-for-economic-co-operation-and-development-oecd-global-tax-deal-global-tax-deal/
[68] https://kluwertaxblog.com/2025/01/29/the-global-tax-deal-memorandum-is-another-wake-up-call-for-europe/
[69] https://unctad.org/system/files/official-document/der2019_en.pdf
[70] https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/10/understanding-the-potential-scope-definition-and-impact-of-the-wto-e-commerce-moratorium_1a15ea94/59ceace9-en.pdf
[71] https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3982
[72] https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/09/economic-implications-of-data-regulation_7a6a28ba/aa285504-en.pdf
[73] https://single-market-economy.ec.europa.eu/smes_en
[74] https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf
[75] https://neweconomics.org/uploads/files/NEF_DATA-INADEQUACY.pdf
[76] Alan O Sykes, The Law and Economics of "Forced" Technology Transfer and Its Implications for Trade and Investment Policy (and the U.S.–China Trade War), Journal of Legal Analysis, Volume 13, Issue 1, 2021, Pages 127–171, https://doi.org/10.1093/jla/laaa007
[77] https://www.meti.go.jp/english/report/data/2020WTO/pdf/column_06.pdf
[78] https://www.economist.com/business/2025/03/13/western-companies-are-experimenting-with-deepseek
[79] https://www.politico.eu/article/europe-looks-to-follow-on-tackling-risk-of-chinese-car-software/
[80] https://www.globaltimes.cn/page/202411/1323469.shtml
[81] https://www.turing.ac.uk/sites/default/files/2021-06/dorobantu_ostmann_hitrova_2021_1.pdf
[82] https://www.cigionline.org/sites/default/files/documents/no239_2.pdf
[83] Borghi, Maurizio and White, Benjamin, Data Extractivism and Public Access to Algorithms (January 1, 2023). Law, Regulation and Governance in the Information Society: Informational Rights and Informational Wrongs, pp 105-125, 2023, DOI: 10.4324/9781003242987-7, Available at SSRN: https://ssrn.com/abstract=4771780
[84] https://www.lexology.com/library/detail.aspx?g=f5b1193c-f423-4f96-bca5-03f5145ecf15
[85] https://www.cigionline.org/static/documents/no.295.pdf
[86] Ibid.
[87] Godfrey, Joseph, Who's Afraid of Reverse Engineering? (February 23, 2024). 1 Intellectual Property Quarterly 50 [2024], Available at SSRN: https://ssrn.com/abstract=4853741 or http://dx.doi.org/10.2139/ssrn.4853741
[88] These follow the EU's non-paper on *Model Clauses for negotiation or re-negotiation of Member States' Bilateral Investment Agreements with third countries*. https://edit.wti.org/document/show/74fa928b-21bd-4ff6-b80d-e21dda7e13c7
[89] https://forms.justice.govt.nz/search/Documents/WT/wt_DOC_178856069/CPTTP%20W.pdf
[90] https://www.bsg.ox.ac.uk/sites/default/files/2024-10/Policy%20brief%20-%20AI%20governance%20and%20the%20future%20of%20digital%20trade%20policy.pdf
[91] https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/singapore/eu-singapore-agreements/agreements-explained_en
[92] https://ec.europa.eu/newsroom/just/items/627665/en
[93] https://www.edps.europa.eu/data-protection/our-work/publications/opinions/2025-03-21-edps-opinion-42025-proposals-council-decisions-signing-and-conclusion-behalf-union-digital-trade-agreement-between-european-union-and_en
[94] Yakovleva, Svetlana and Irion, Kristina, Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation (January 06, 2020). (2020) 114 AJIL Unbound 10, 10-14, DOI: 10.1017/aju.2019.81, Available at SSRN: https://ssrn.com/abstract=3524245
[95] https://academic.oup.com/jiel/article/27/3/397/7718688
[96] https://www.citizen.org/wp-content/uploads/WTO-General-Exceptions-Paper_-1.pdf

NOTES

NOTES

The Left in the European Parliament
Rue Wiertz 43 B-1047 Brussels
www.left.eu