EDRi 20
European Digital Rights

Digital Trade Agreements:

A Trojan Horse for Weaker Protections?

Background Paper on the EU's Digital Trade Agenda

April 2025

Published in Brussels, 30 April 2025.

Lead author: Itxaso Domínguez de Olazábal

European Digital Rights (EDRi) is sincerely grateful to our members and partners - notably Ante Wessels - who supported with the research, conceptualisation, drafting and review of this paper.

Contents page

Executive Summary

The EU is rapidly incorporating digital trade rules into international agreements, with the Digital Trade Agreements (DTAs) with Singapore and Korea marking the first of their kind. While these agreements are framed as tools for fostering economic growth and regulatory cooperation - and this could indeed be the case if they are well and carefully designed - they also risk creating avoidable threats, particularly when it comes to the protection of people's rights. EDri has long mantained that Free Trade Agreements (FTAs), especially if not designed with sufficient safeguards, may not be appropriate instruments for governing critical areas such as privacy, data protection, and AI and software-related oversight, amongst others. Despite these challenges, the EU has chosen to integrate these issues into its FTAs and design new DTAs, raising concerns that certain provisions could limit the bloc's ability to adapt laws to evolving technological risks and societal harms.

By committing to broad data flow provisions without ensuring adequate safeguards, and by introducing restrictions on software oversight, **these agreements risk setting problematic precedents for current and future trade negotiation**s. **DTAs,** following the example set by digital chapters in FTAs, **illustrate a broader trend: while digital trade policy holds the potential to harmonise economic interests in line with**

rights-based considerations, the inclusion of provisions that do not belong in such agreements - combined with the vague and harmful way in which they are currently worded - poses a serious threat to fundamental rights. If not carefully reviewed and crafted, such agreements could leave the EU unable to effectively defend human rights, with its actions unduly constrained by trade obligations and the limitations embedded in trade agreements. The analysis below outlines key concerns and provides recommendations for policymakers engaged in these processes.

1. Lack of Regulatory Flexibility and Autonomy

- The agreements with Singapore and Korea (and potentially others in the future) lack full coherence with the EU's existing digital rulebook. This raises critical questions about whether DTAs could undermine the enforcement and future evolution of key EU regulations by imposing trade commitments that restrict regulatory flexibility, autonomy and action.
- Although DTAs include certain critical exceptions, their limitations are well-documented - as outlined in the section on 'Why Exceptions Don't Work'. These carve-outs offer little assurance in practice, and could undermine the EU's ability to regulate effectively. Moreover, **trade agreements are inherently designed to limit the scope of EU regulation in favour of facilitating trade,** meaning that even with exceptions, the overall framework tends to restrict regulatory flexibility which can disempower the EU's ability to protect and promote fundamental rights.

2. Data Flows & Data Protection and Privacy Risks

- The agreements could commit the EU to potentially unrestricted cross-border data flows with third countries, while providing insufficient and ambiguous safeguards for the fundamental rights of data protection and privacy, and more broadly limiting the full application of the EU Data Governance framework.
- The lack of an adequacy decision in the case of Singapore is problematic: the country's weak privacy laws and extensive state surveillance practices raise significant risks for EU individuals' data, potentially exposing it to misuse, including from third countries with fewer safeguards. In the case of the DTA with Singapore, the EDPS' Opinion 4/2025 echoes some of these concerns about the provisions on data flows.
- The EU has already established mechanisms to regulate data flows, making trade agreements an inappropriate and inadequate forum for such regulation.

- **3. Barriers to Software Oversight & Algorithmic Accountability**
  - **The bans on requiring access to source code in DTAs** so far, despite carve-outs theoretically allowing access by public authorities, **could severely limit the EU's ability to audit not only AI systems but also other software-based solutions.** This limitation could weaken enforcement of digital laws and the fundamental rights they protect, whilst also failing to account for future regulatory innovation which would allow the EU to further protect people's rights.
  - Notably, **these restrictions could obstruct the enforcement of the AI Act, which requires certain access to algorithms to assess bias, discrimination, and systemic risks, as well as other critical laws in the EU's digital rulebook.** They could also affect laws that are not strictly digital in nature but are crucial for ensuring that software-based solutions respect fundamental rights. It could have significant consequences for the rights of communities in positions of power imbalances, including workers' rights, by limiting regulators' - and others' - ability to scrutinise automated decision-making systems.
- **4. Opaque Negotiation Process & Lack of Public Scrutiny:** the negotiations of these DTAs so far have been highly opaque, with extremely limited stakeholder input and very limited transparency.

Introduction

The European Digital Rights (EDRi) network has long advocated for a balanced and rights-respecting approach to digital trade. While digital trade can facilitate Europe's economic growth and international cooperation, EDRi has consistently cautioned against including sensitive digital policy provisions within trade agreements, particularly without adequate safeguards. As outlined in the TACD 2019 Resolution on Digital Trade, trade deals are not the appropriate forum for addressing every aspect of digital policy. Currently, 91 World Trade Organisation (WTO) Members - including the EU, which participates on behalf of all EU Member States - are engaged in e-commerce negotiations aimed at harmonising digital trade rules.

However, these efforts often lack the necessary safeguards to ensure that fundamental rights, such as data protection and privacy, and regulatory autonomy, are not compromised. A notable policy shift occurred in October 2023 when the Office of the U.S. Trade Representative withdrew the U.S. support for provisions related to data

flows, and source code, mentioning how these provisions could potentially mean 'massive malpractice' and even 'policy suicide'. With a new U.S. administration now in power, and in an epoch of tariff bullying and growing efforts to carve out exceptions for Big Tech, trade is becoming more central - and more contested - than ever. In this context, the EU must reaffirm its commitment to global fundamental rights - ensuring that digital trade negotiations do not undermine existing protections.

The emphasis on digital provisions in a new wave of bilateral and multilateral FTAs or stand-alone DTAs, at a time when deregulation appears to dominate the EU's agenda, reveals how trade agreements play a key role in international economic governance but without sufficient safeguards, may function as instruments of transnational rulemaking aimed at deregulation itself. They can constrain policy and regulatory autonomy, even when they seem to include some prima facie positive provisions. Central to the EU's digital trade agenda is a delicate balance between economic competitiveness and fundamental rights. However, there is an increasing risk that economic interests are being prioritised at the expense of robust protections, when in fact, **economic interests must always operate within the playing field of fundamental rights and EU values.** Despite these far-reaching implications, **the European Commission has not yet provided clear explanations on how digital trade commitments align with its own legal framework**. This lack of clarity raises serious questions about the consistency of the EU's approach and its ability to enforce its own digital laws without being constrained by trade obligations.

Previous agreements, such as the EU-Japan Deal on Data Flows, exemplify these challenges. The framework has faced scrutiny for its insufficient alignment with EU data protection standards, echoed by the EDPS, and its failure to address Artificial Intelligence (AI) oversight, along with broader digital rights concerns. Many aspects of this deal have been replicated in subsequent EU agreements. These provisions are expected to serve as a foundational step towards establishing a common approach to digital trade, whether in separate DTAs or through the inclusion of digital trade chapters in free trade agreements with countries with which the EU is already negotiating similar agreements. This includes the Philippines and Thailand.

This paper critically examines the EU's broader digital trade agenda, with a particular focus on the recently concluded EU-Singapore and EU-Korea DTAs. **EDRi recognises the importance of fostering digital trade but stresses the need for robust safeguards to ensure regulatory autonomy and fundamental rights are upheld.** We have reviewed the pre-legal scrub version of the Singapore DTA, set to be ratified by Council and European Parliament. While some provisions may offer benefits, others

intensify existing concerns, outweighing any potential benefits. This is particularly significant because the EU-Singapore DTA represents the first stand-alone EU digital trade agreement of its kind, potentially serving as a model for future deals with other ASEAN countries and beyond. These concerns are even more pressing in the context of the EU-Korea DTA, whose completion was announced on 9th March 2025. At the time of writing, EDRi has not yet had access to the text of the latter agreement.

As the EU and its trade partners move toward the formal adoption of these DTAs, EU institutions have a critical responsibility to ensure that DTAs complement - rather than undermine - fundamental rights protections. This paper underscores the urgency for the EU to embrace a leadership role in addressing the recommendations outlined below. These concerns are shared by other EU Civil Society Organisations, such as BEUC and ETUC, as well as researchers and experts in computer science.

EDRi has repeatedly highlighted the far-reaching implications of provisions on cross-border data transfers and access to source code within trade agreements. These provisions impact not only data protection and algorithmic discrimination but also intersect with crucial areas such as the future of work, freedom of expression, and issues related to both commercial surveillance and state surveillance. While DTAs can facilitate economic cooperation, it is essential that they do not erode fundamental rights in the process. This Background Paper outlines critical concerns regarding these DTAs, particularly in relation to these provisions. It argues that the DTAs risk disproportionately prioritising economic interests over fundamental rights and democratic accountability, setting a troubling precedent for future trade agreements.

All trade agreements are binding and notoriously difficult to revise once signed. That’s precisely why digital trade rules must be approached with caution. Even if current conditions seem acceptable, the real test is how these rules hold up when things change - when new technologies appear, when power dynamics shift, or when enforcement is politically inconvenient. What looks harmless today can become a serious barrier to regulation tomorrow. So the key question in any negotiation isn’t just whether the rules work now, but whether they can prevent harm - or be misused - in the future. **The EU's negotiation process has further exacerbated these issues, marked by limited transparency and restricted public access to negotiation texts.** This opacity undermines democratic legitimacy and raises questions about undue corporate influence over policymaking, particularly in a field like digital trade where negotiations often reflect the priorities of large technology firms. The lack of transparency in mandate-setting and stakeholder consultations can allow dominant industry actors to

shape provisions in ways that prioritise market access and deregulation over fundamental rights, public interest safeguards, and the perspectives of civil society, workers, and marginalised communities. While economic benefits are heavily emphasised, the potential impact on fundamental rights remains insufficiently addressed. This paper examines the most problematic provisions of the DTAs agreed so far, offers recommendations, and includes an Annex with a detailed analysis of the corresponding provisions and context of the EU-Singapore DTA. A second Annex will be added once access to the text of the EU-Korea DTA has been secured.

Recommendations

DTAs must prioritise public interest and ensure the protection of people's rights. They must not hinder the EU's ability to enforce its digital laws or prevent member states from exceeding minimum EU standards where necessary. Moreover, **DTAs should safeguard - not constrain - the policy space needed to adopt and strengthen regulatory and other measures in response to evolving challenges** in the digital economy.

In this context, the European Commission must take into account these recommendations when negotiating future texts, ensuring that they uphold fundamental rights and public interest. **The European Parliament should propose amendments to the existing Singapore and Korean texts as conditions to ratify them, furthermore ensuring that any future agreement aligns with the EU's regulatory framework.** Finally, the Council should review the final agreements closely during the ratification process and, if it finds that the agreement fails to protect key EU interests and protections as outline in this paper, should reject it, ensuring that the EU's regulatory autonomy and commitment to human rights are preserved. This includes a need to:

- Ensure Coherence with EU Law
  - The European Commission should conduct a mandatory coherence assessment for each DTA, involving DG TRADE, DG CONNECT, and DG JUST, and publish the results before finalising any agreement.
  - This assessment must identify gaps or contradictions with the GDPR and the complete digital rulebook, including the Data Act and the Data Governance Act and other laws that could be impacted by the human rights impact of software-based solutions.
  - All such assessments must involve meaningful public consultations, with civil society, academia, and regulators.

- The European Commission should also guarantee the transparency of negotiation documents, ensuring that they are accessible to the public in a timely manner.
- The EU must refrain from including provisions on cross-border data flows and source code access in future trade agreements, as these clauses pose serious risks to regulatory autonomy and fundamental rights. If, despite these risks, such provisions are retained, their wording must be meticulously reviewed and significantly redrafted to ensure they do not undermine existing digital legislation. Please see below.

- Prioritise High Data Protection and Privacy Standards
  - If the inclusion of provisions on data flows. is maintained despite the warnings raised in and beyond this paper, legislators must reinstate the 2018 horizontal provisions on cross-border data flows and personal data protection in their exact wording, both when it comes to data protection and privacy as EU fundamental rights, as a non-negotiable red line.
  - The EU-Singapore DTA should explicitly supersede the implicit data flow commitment in the EUSFTA.
  - The European Commission should prioritise adequacy decisions with trading partners to ensure that data flows meet the highest standards of data protection. Adequacy and other mechanisms in Chapter V GDPR should be pursued as a stand-alone mechanism outside trade agreements.
  - Data protection and privacy must be excluded from dispute settlement mechanisms and trade balancing tests.

- Ensuring Accountability and Transparency of Software-Based Solutions
  - The European Commission should conduct a comprehensive review of the provisions related to source code in its trade agreements, similar to the recent recommendation from the UK House of Lords International Agreements Committee.
  - DTAs must not include provisions that restrict or condition public authorities' ability to demand access to source code or algorithmic logic.
  - If such provisions are included, they must be redrafted to guarantee unambiguous rights for public oversight and legal enforcement.
  - DTAs should affirm - not merely acknowledge - the unconditional right to regulate in the public interest, particularly on digital rights.

By implementing these recommendations, the EU can ensure that DTAs uphold democratic accountability, safeguard fundamental rights, and prevent undue corporate or governmental influence in policymaking. This

approach will help set a global benchmark for responsible and rights-respecting digital trade frameworks. This is even more crucial in a time when trade wars are likely to become more frequent, as geopolitical tensions increasingly shape economic policies. Ensuring that DTAs prioritise fundamental rights and regulatory autonomy will be essential to prevent powerful actors from using trade disputes as leverage to weaken EU digital laws. Without strong safeguards, there is a real risk that economic pressures could erode hard-won protections, leaving individuals and democratic institutions vulnerable to undue external influence and corporate capture.

It is critical for us to emphasise that this is not about imposing the General Data Protection Regulation (GDPR) or any other aspect of the EU's digital rulebook on other countries, nor about compromising trade secrets or undermining intellectual property rights. Rather, it is about ensuring that all nations retain the capacity to regulate in the public interest, protecting the rights to privacy, data protection, and other fundamental rights for individuals and communities alike. It also seeks to ensure that people’s data is safeguarded when transferred to third countries with which the EU establishes trade agreements. Ultimately, the aim is to uphold well-established fundamental rights both within the EU and globally, while promoting trust in the digital economy and enhancing the integrity of international trade.

While this document focuses on the implications of DTAs for EU digital regulation, it is essential to recognise that the impact of such agreements extends beyond the EU legal framework. The provisions within the DTAs will also shape the digital rights landscape in Singapore and Korea, and may have broader consequences for affected individuals and communities, including workers, consumers, and marginalised groups both within and beyond the contracting parties. A more comprehensive assessment of these agreements should take into account not only their effect on EU regulatory autonomy but also their potential to exacerbate or mitigate digital inequalities, corporate power asymmetries, and state surveillance practices in the respective third countries. Further analysis is needed to fully understand these dimensions and ensure that digital trade policies do not entrench harmful structures or undermine human rights globally.

Why Exceptions Don’t Work: Trade Law’s Weak Safeguards

Trade Agreements include clauses that ostensibly allow governments to restrict data flows or demand access to source code where necessary to

protect public interest. This is a welcome and necessary inclusion. However, in practice, these exceptions are often weak, narrowly defined, and legally unreliable.

Many of these carve-outs rely on what is known as a necessity test, a trade law principle requiring states to prove that their measures are the least trade-restrictive way to achieve a legitimate public policy goal. This is a high and often insurmountable threshold. A historical review shows that only 2 out of 48 attempts to invoke such exceptions under the GATT and GATS frameworks have succeeded.

Other exceptions are framed using non-discrimination clauses, which prohibit ‘arbitrary or unjustifiable discrimination’ or ‘disguised restrictions on trade’. While they seem broader, they still leave too much interpretative power in the hands of dispute resolution bodies and rarely prioritise fundamental rights over trade facilitation.

Even when exceptions are framed around the protection of ‘legitimate public policy objectives’- such as public health, public security, or environmental protection - they remain problematic. Although these references may seem less restrictive at first glance than the strict necessity test, they still operate within a trade law logic that privileges market access. Their interpretation might be subject to dispute resolution panels that often prioritise trade liberalisation over fundamental rights. In practice, governments must still demonstrate that their measures are not only necessary but also non-discriminatory, proportionate, and the least trade-restrictive means available, which imposes a heavy evidentiary burden. This risks discouraging the adoption of rights-protective regulations by creating uncertainty about whether such measures would survive a potential trade challenge.

These limitations apply across both source code secrecy provisions and cross-border data flow clauses, analysed below. In both cases, the real-world effect is that governments - including the EU and its Member States - face legal ambiguity and potential liability when enacting or enforcing human rights protections that may affect trade.

This makes **exceptions ill-suited as safeguards for rights-based governance: they introduce risk, uncertainty, and delay in situations that demand clarity and accountability**. Therefore, while trade agreements may affirm the ‘right to regulate’, this right is qualified and weakened by the architecture of trade law itself. Exceptions should therefore not be used as fig leaves to justify the inclusion of provisions that fundamentally constrain rights-based governance in digital contexts.

The Perfect Storm: How Data Flows Provisions and Source Code Secrecy Undermine Digital Rights

Below you can find an analysis of the problematic aspects of the provisions allowing for cross-border data flows and prohibiting access to source code. It is critical to acknowledge how these provisions intersect in ways that can significantly impact digital rights.

Regulatory Forgotten Elements and Corporate Secrecy: the provisions facilitating free data flows enable companies to transfer vast amounts of personal and non-personal data to countries with weaker privacy and data protection protections (Singapore and others - see below). At the same time, prohibitions on source code disclosure prevent regulators, researchers, and civil society from scrutinising the algorithmic systems that process this data. This creates a regulatory gap where companies can operate with minimal oversight, making it harder to detect harmful practices.

Limits on AI and Algorithmic Accountability: the combination of potentially unrestricted data flows and protected source code secrecy reinforces the opacity of AI-driven decision-making. If companies can freely transfer personal and other kinds of data while keeping their algorithmic models hidden, affected individuals and regulators lose the ability to audit or challenge discriminatory and other human rights-affecting decisions. This worsens concerns around 'black box' systems, where neither the logic nor the datasets shaping decisions can be meaningfully examined.

Risks of Regulatory Arbitrage and Forum Shopping: if companies can store and process data in jurisdictions with weaker privacy and data protection protections while simultaneously keeping their AI models and other software-based solutions inaccessible to regulators, they can effectively bypass accountability measures. This creates incentives for *forum shopping*, where businesses relocate data processing activities to avoid regulatory oversight. The EU might still impose obligations on companies operating within its territory, but enforcement would be severely weakened without access to the underlying source code and decision-making logic.

Regulating AI and Software in the Dark: How Source Code Prohibitions Could Shield Harmful Practices

The inclusion of AI and software governance provisions - a clause that 'enables an internet of cheating things' - in trade agreements is deeply problematic. These agreements are ill-suited to address the nuanced ethical, societal, technical, and human rights-related, challenges posed by AI systems, models, and software-based solutions. Effective governance requires targeted regulation that prioritises rights, transparency, accountability, and societal impact - issues that cannot be meaningfully addressed within the confines of trade frameworks. This need becomes even more pressing as increasingly advanced foundation models emerge, and the widespread deployment of generative AI accelerates.

Despite these limitations, some countries have linked AI- and software-related provisions to contentious matters, such as prohibitions on source code disclosure, often using standardised clauses copied across agreements with minimal adaptation. This is problematic because it imposes rigid trade disciplines on fast-evolving and highly context-dependent technologies, without accounting for local regulatory needs, public interest safeguards, or the specific risks posed by AI systems. Such one-size-fits-all provisions can constrain the ability of governments to ensure transparency, accountability, and human rights protections in the development and deployment of these technologies.

This approach has faced significant criticism, including from the UK House of Lords International Agreements Committee, which has called for a comprehensive review of such clauses, particularly focusing on their exceptions. The widespread adoption of these provisions risks undermining not only AI-specific governance but also broader digital rights enforcement by prioritising trade facilitation over the protection of fundamental rights. The EU should adopt a similar review process to ensure that trade agreements do not weaken the governance of AI and software-based systems, particularly in ways that could reinforce structural discrimination or other human rights violations.

The main concern with banning disclosure of source code: limitation of accountability

These mechanisms are often framed as necessary protections against 'forced' disclosure by foreign governments[1], ostensibly to safeguard intellectual property and trade secrets. However, in practice, such provisions create significant regulatory forgotten elements, shielding not just AI-driven systems but also broader software solutions that shape decision-making in critical areas such as hiring, social welfare, law enforcement, and financial services. By preventing access to source code and key technical documentation, these clauses risk turning essential automated processes into 'black boxes', making it harder to assess bias, discrimination, and other systemic harms. This has profound implications for the regulation of software-driven decision-making, not only within the EU and Singapore but globally.

While these provisions are often justified as measures to prevent the extortion of confidential business secrets, it is important to recognise that **actors and governments already engaged in such practices will likely continue regardless of trade agreement clauses.** Instead of addressing unfair or coercive demands for proprietary data, these restrictions severely limit the transparency required to ensure responsible governance of both AI and other software-based decision-making tools. They impede efforts to examine whether automated processes - such as hiring software, fraud detection systems, or predictive policing tools - are reinforcing institutional biases, structural discrimination, or other human rights violations.

Crucially, t**hese provisions extend beyond protecting legitimate trade secrets**. By broadly shielding all source code - even that which does not qualify as confidential business information - the DTAs layer unnecessary barriers to oversight. Source code is more than just programming instructions; in software-driven decision-making, it encodes rules, assumptions, and logics that define how systems function, process data, and produce outcomes. For AI-based and non-AI-based tools alike, access to source code allows regulators, auditors, and other stakeholders to scrutinise whether systems operate lawfully, and in compliance with fundamental rights. Without such access, it becomes significantly harder to hold the developers and deployers of automated decision-making systems accountable for discriminatory outcomes, privacy violations, or flawed decision-making, whether the system is explicitly AI-driven or not.

[1] It is worth noting that the governments which actually employ this approach have not agreed to treaties that include provisions on source code.

The absence of a definition[2] for the key term 'source code of software' further exacerbates these issues. This ambiguity creates space for varying interpretations, raising serious concerns about its practical application. It remains unclear whether the provision covers only raw code or extends to critical elements such as algorithms, machine learning models, or datasets that shape software behaviour - including the provenance and quality of training data. Even in non-AI systems, embedded assumptions and rule-based decision-making frameworks can perpetuate harm, making regulatory scrutiny essential across the entire system. This lack of clarity may allow dominant actors to interpret the provision in ways that restrict oversight and transparency, potentially enabling the evasion of accountability mechanisms designed to safeguard fundamental rights.

Locking in rigid source code protections within a trade agreement also severely limits the EU's ability to respond to future technological developments. Software systems - whether AI-based or not - are evolving rapidly, and what is considered 'source code' today may not fully encompass emerging components that drive decision-making, such as dynamic rule-based engines, decision trees, or hybrid AI-human systems. A narrow interpretation of the provision could prevent regulators from scrutinising these increasingly influential architectures, effectively constraining their ability to mitigate systemic risks. By embedding such constraints in a trade framework, the EU risks losing the regulatory flexibility needed to adapt to new challenges, while allowing powerful actors to shield opaque and potentially harmful systems from public scrutiny.

Moreover, the reference to 'legitimate policy objectives' does little to mitigate these concerns. As explored in 'Why Exceptions Don't Work', vague references to legitimate policy objectives might not ultimaltely provide enforceable safeguards.

When public authorities are denied access to source code, the ability to hold corporations and public authorities accountable for harm caused by automated decision-making - whether AI-driven or not - is significantly undermined. Whether embedded in AI systems or traditional software, opaque decision-making tools can facilitate privacy violations, discriminatory practices, and censorship. Without transparency, independent experts, civil society organisations, and regulators may struggle to detect and address these harms. This opacity threatens to entrench systemic discrimination and unchecked corporate power, making it harder to

[2] In this scenario, the interpretation of the treaty would be governed by the principles outlined in the Vienna Convention, which would require that the provision's wording shall be understood according to its plain and ordinary meaning, while also considering the broader context in which the terms are used and the overall aims and objectives of the agreement. See https://dl.acm.org/doi/fullHtml/10.1145/3531146.3533212

ensure that software-driven decision-making operates in a fair, lawful, and rights-respecting manner.

Transparency is a fundamental pillar of both AI and software governance, enabling regulators and the public to scrutinise how automated systems function and whether they reinforce harmful biases. Without meaningful oversight, discriminatory algorithms, exploitative practices, and human rights violations may remain undetected and unchallenged.

Potential Negative Impacts on EU Digital Legislation

By introducing an additional layer of protection for source code - without adequately addressing the shortcomings outlined above - the EU risks reversing the proper sequence of digital lawmaking. In this approach, trade agreements establish the foundational framework, forcing digital regulation to adapt accordingly. This dynamic prioritises economic and commercial interests over the fundamental rights and regulatory principles that should shape digital policymaking.

Unlike the blanket protection introduced in these provisions, the EU's current legal framework does not treat all source code as inherently protected. Instead, source code may fall under copyright law or be safeguarded through the EU Directive on Trade Secrets, both of which impose specific conditions. By establishing new protections without linking them to these existing legal structures, the provision creates an independent and overly broad layer of defence. This not only adds unnecessary complexity but also disrupts the balance of the existing framework, which includes public interest exceptions . These exceptions to IP rights play a critical role in ensuring that transparency, accountability, and the protection of fundamental rights are not sidelined in favour of commercial secrecy.

Crucially, **this provision does not solely affect AI systems but extends to all software-based solutions, including those that structure decision-making in hiring, welfare distribution, and public services[3]. Software, even without AI, can embed and reinforce institutional biases, leading to discrimination and other rights violations.** By shielding source code from scrutiny, the provision could significantly hinder

[3] It's worth pointing that the definition of AI was a key point of contention throughout the negotiations of the AI Act. Industry actors consistently pushed for a narrow, technocraticical definition that would limit the scope of the rules and reduce compliance obligations. In contrast, digital rights advocates called for a broader, more functional definition that captures a wider range of systems with real-world impacts, arguing that only a broad scope can ensure meaningful protections for individuals and communities affected by AI models and systems.

EU and national authorities in implementing and enforcing digital regulations, making it more difficult to safeguard the rights and interests of individuals and collectives across the EU. This issue extends beyond AI systems, affecting a broad range of digital regulations where transparency and accountability hinge on access to source code. This would be the case with the following, as well as consumer protection laws:

- This would be the case with Digital Services Act (DSA), which imposes obligations on online platforms to ensure transparency and accountability in the way they moderate content, target users with advertisements, and recommend information. Without access to source code, regulators and oversight bodies may struggle to assess whether platforms' algorithms comply with the DSA's requirements, such as mitigating systemic risks or ensuring algorithmic transparency. This lack of oversight could undermine the enforcement of critical safeguards against misinformation, hate speech, and other societal harms.
- In the case of the EU-Singapore DTA, the clause's vague requirement for 'proportionate and targeted' access to source code could hinder the enforcement of the Digital Markets Act (DMA) by introducing legal uncertainty over regulators' ability to scrutinise gatekeepers' algorithms and ranking systems. Without a clear definition, dominant platforms could challenge requests for access, delaying investigations into self-preferencing and non-compliance with interoperability obligations. This ambiguity risks weakening the European Commission's enforcement powers, as companies may argue that broad or systematic access - essential for proactive compliance monitoring - is disproportionate, ultimately obstructing efforts to ensure fair and competitive digital markets.
- The same concerns apply to the General Data Protection Regulation (GDPR), which grants individuals subjected to automated decision-making processes - including profiling - the right to meaningful information about the logic involved. This requires transparency in how algorithms process personal data to make decisions, as confirmed by the CJEU in Case -203/22. A blanket restriction on source code disclosure could significantly impair regulators' and data subjects' ability to examine these systems, identify privacy breaches and discriminatory patterns, or challenge unfair outcomes. Whether AI is involved or not, this lack of transparency would severely limit the GDPR's effectiveness in safeguarding individuals from opaque and potentially unlawful data processing.
- Most notably, this issue also applies to the Artificial Intelligence Act (AI Act). It is no coincidence that legislators were compelled to scale back their regulatory ambitions, in part to align with the source code provisions stipulated in trade agreements. This adjustment reportedly occurred after negotiators were informed by the European Commission's

trade department that the inclusion of such provisions would directly conflict with the AI Act's transparency and accountability requirements, highlighting the exact tension between international trade commitments and robust AI governance against which we warn.

- The AI Act demands that high-risk AI systems are subject to a level of scrutiny that includes access to the underlying algorithms and source code for market surveillance authorities in certain circumstances (Article 74.13). This is essential for regulators to assess whether AI systems are functioning as intended, particularly in relation to ensuring that they do not violate human rights. If the EU-Singapore DTA restricts access to source code, it could undermine the EU's ability to enforce the AI Act effectively. Without access to source code, it would be challenging, if not impossible, for regulators to perform the necessary assessments of high-risk AI systems that are required by the AI Act.

Other potential negative impacts of the provision

As algorithmic decision-making becomes increasingly prevalent, more and more decisions - especially business-related ones - are being driven by AI systems and software-based solutions. However, when access to source code is potentially restricted, it poses a significant challenge, as it removes the transparency needed to ensure these decisions are rights-respecting, accountable, and free from discrimination. Decisions made by both public authorities and private companies can significantly affect individuals and society at large - but while the state bears the greatest responsibility to uphold rights and ensure accountability, corporate actors must also be subject to robust oversight.. By keeping the source code potentially inaccessible, there is a risk of shielding the very systems that need the most scrutiny, making it difficult for regulators and civil society to understand how and why certain decisions are made.

- Threats to workers' rights. The prohibition could also pose significant risks to workers' rights, particularly in the context of algorithmic discrimination. As shown by numerous investigations, AI systems, including those used in hiring, performance evaluations, and workplace monitoring, can perpetuate bias and discrimination, particularly when because underlying algorithms are not transparent or subject to scrutiny. Non-AI digital tools used in labour management can pose similar risks. Without access to the source code, there is no way for workers, trade unions, or regulators to assess whether algorithms are discriminating based on gender and gender identity, race, age, or other protected characteristics. This lack of oversight could surely lead to systemic inequalities in the workplace, where decisions are made by

opaque algorithms that adversely affect workers, even more so those coming from marginalised communities, limiting their opportunities for advancement or even leading to unfair dismissals. The absence of accountability in AI systems could thus undermine workers' rights to fair treatment, equal opportunity, and protection from discrimination. Furthermore, by shielding these systems from public and regulatory scrutiny, the agreement effectively prevents the introduction of safeguards or corrective measures that could protect workers from algorithmic harm, reinforcing a power imbalance that favours employers and companies over employees.

- Limits to freedom of expression. Moreover, source code is a medium through which digital tools and platforms can be developed to express ideas and enable communication. Prohibitions on source code could prevent individuals or organisations from creating software that supports freedom of expression or promotes democratic values. This is especially relevant in countries where governments may want to prevent the creation of tools that support dissent, freedom of speech, or access to information.

- Limits to right to redress. This provision could create significant barriers to justice for individuals who have suffered harm due in part to the use of AI systems and other software-based mechanisms, making it nearly impossible for them to seek appropriate redress. In trade agreements, clauses that prioritise the free flow of data and the protection of business interests often shield companies from legal responsibility, while providing few, if any, avenues for affected individuals to hold them accountable. As a result, when individuals suffer damage - such as discrimination, privacy and data protection violations, or physical or financial harm due to flawed AI systems and other software-based solutions - they may face substantial legal and procedural hurdles in proving the harm. Such scenarios would exacerbate the power imbalance between corporations or public entities and individuals, particularly in the realm of emerging technologies, where potential risks to human rights are often not fully understood or addressed. Without adequate mechanisms for accountability and justice, these issues could remain unresolved, deepening the gap between technological progress and the protection of fundamental rights.

- Reinforcing the power of Big Tech. The provision also risks creating a regulatory environment where private companies - especially large multinational tech firms - hold disproportionate power over software-based development and deployment. Without the ability to inspect or demand modifications to source code, governments may be unable to implement safeguards that ensure some systems align with fundamental rights.

- Constraining International Cooperation. The prohibition on access to source code in trade agreements could risk severely constraining international collaboration on AI governance. By shielding the inner workings of AI and other software-based technologies from regulatory oversight, this provision could create barriers to collaboration, allowing rights-violating practices to proliferate unchecked across borders.
  - This concern becomes particularly alarming when viewed in the context of recent efforts by the EU and Singapore to bolster cooperation on AI safety. Notably, the two parties have signed initiatives such as the EU-Singapore Digital Partnership and a specific arrangement on AI cooperation. While these instruments aim to promote the ethical development and use of AI systems, they are non binding and lack the legal enforceability and institutional oversight that characterise trade agreements. It raises the question: how can such cooperation on AI safety be reconciled with a provision in the DTA that effectively restricts access to source code - the very foundation of AI technologies?

- Fewer opportunities for innovation. Finally, restricting access to source code could limit opportunities for innovation over time. The ability to inspect, modify, and improve source code is essential for advancing secure, rights-respecting, and effective AI systems and other software solutions. When requirements for source code disclosure on an open source basis are introduced, it can play a significant role in promoting innovation and economic growth. Sharing source code with other organisations can drive the adoption of new technologies, stimulate further inventions, ensure that different technology solutions work together seamlessly, and help grow the industrial ecosystem. However, by restricting such access, the EU-Singapore DTA could unintentionally hinder the development of technologies that are crucial for safeguarding fundamental rights.

Data Without Borders, Rights Without Guarantees: The Risks of Digital Trade Rules on Data Flows

Provisions promoting the free flow of data in DTAs, like those included in the EU-Singapore and EU-Korea DTAs, are problematic for several reasons, especially taking into account that **they undermine not just the fundamental rights to privacy and data protection, but also other fundamental rights attached to it.** The inclusion of these clauses is often driven by extensive lobbying from Big Tech companies, which are eager to secure unhindered data transfers to further their business interests.

While these provisions are theoretically designed to provide legal certainty for cross-border digital services and advance economic interests, what could they end up doing is severely restricting governments' ability to regulate data flows based on their own public policy needs and in ways that protect individuals and collectives' rights. Rather than harmonising the EU's single market, this can conversely increase fragmentation. In the case of the DTA with Singapore, the EDPS' Opinion 4/2025 echoes some of these concerns regarding the provisions on data flows. While the agreements includes exceptions meant to safeguard data protection, these safeguards remain insufficient to fully guarantee the EU's regulatory autonomy. The broad commitments to data transfers risk conflicting with the EU's fundamental rights framework.

EDRi and other civil society organisations have repeatedly argued that data protection and privacy, and data flows generally, should be entirely excluded from trade agreements, with the EU's data protection and privacy framework taking precedence. As already mentioned, **trade agreements are inherently rigid and difficult to amend, unlike domestic laws, which can be changed through common legislative process**. This rigidity means that if a party breaches the terms of a trade agreement, it could face penalties, sanctions, or other enforcement actions. This creates a scenario where evolving domestic needs, such as the need to enhance data protection and privacy laws in response to new challenges, or the need to implement them in different ways if the need arises, might be subordinated to the priorities of the trade agreement, in effect forcing the EU's hand. The inclusion of clauses that restrict data regulation can lead to situations where governments, and thus also the EU and its regulators, face challenges when trying to implement or enforce laws that protect data, be it personal data or not.

Building on these concerns, the independent 2016 study commissioned by EDRi, BEUC, TACD, and the Center for Digital Democracy underscored the **significant risks posed by the inclusion of data-related provisions in trade agreements**. It highlighted that trade agreements, such as those negotiated by the EU, could undermine the ability of governments to regulate data protection effectively, especially when conflicting with commercial interests. The study pointed out that provisions enabling the free flow of data across borders can limit the EU's ability to enforce its data protection laws, including the GDPR, when trade partners challenge or ignore such regulations. Moreover, the study revealed how trade agreements often prioritise economic considerations over human rights protections, creating a situation where fundamental rights are at risk. As these agreements grow in scope and influence, the long-term effect could be a weakening of the EU's regulatory autonomy, with the overarching power of international trade law potentially rendering privacy and data protection standards increasingly difficult to uphold. This would leave individuals vulnerable to exploitation and surveillance, undermining the core principles of the EU's protection regime

In 2018, the EU Commission adopted a new approach through horizontal clauses on cross-border data flows and personal data protection, introducing broad and strong data flow commitments paired with an unconditional safeguard. This decision marked a significant improvement over earlier ones based on the GATS Article XIV, which imposed conditions such as a necessity test. The explicit recognition of data protection and privacy as fundamental rights in trade agreements was a positive development, welcomed by EDRi and other civil society organisations. The EU applied this 2018 approach in trade agreements with New Zealand (Article 12.5) and Chile (Article 19.6). However, the agreement with the UK fell short of this new standard. The explicit mention of data protection and privacy as a fundamental right was omitted, and alternative formulations were used instead. Disappointingly, the EU has once again opted for weaker safeguards in the DTAs agreement with Singapore (see Annex) and Korea, mirroring the shortcomings of the UK agreement.

While the DTAs might not explicitly derogate from GDPR Chapter V rules, they might do little to ensure the meaningful protection of EU data subjects' rights when their data is transferred to third countries. In practice, although data exporters might remain legally required to comply with GDPR transfer rules, the agreement fails to address the fundamental risks posed by other countries' weak privacy protections (see Annex for the specific case of Singapore). Instead, it risks creating a false sense of security, encouraging businesses and authorities to transfer data without fully considering the legal and human rights implications.

This issue is further compounded by some **DTAs' lack of a clear and enforceable minimum standard of data protection**. Without a requirement for strong safeguards, third countries could continue to operate under weaker and inconsistent data protection frameworks, leaving personal data vulnerable to misuse. Moreover, in the case of countries that do not uphold fundamental rights to an equivalent standard as the EU (see Annex in the case of Singapore), DTAs could serve as a tool to challenge the EU's legal *acquis*, ultimately undermining its ability to enforce robust data protection standards.

The provisions on data flows moreover risk directly undermining the Data Governance Act (DGA) and the Data Act by limiting the EU's ability to control how certain types of data are accessed and shared. The DGA and the Data Act play complementary but distinct roles in the EU's data strategy. The Data Governance Act establishes trusted frameworks for voluntary data sharing, ensuring that sensitive public-sector data, personal data shared for altruistic purposes, and other protected categories are subject to strict conditions. In contrast, the Data Act imposes mandatory obligations on businesses and public sector bodies to share certain types of non-personal and mixed datasets, while introducing safeguards, including restrictions on the international transfer of sensitive data. Both laws are designed to uphold the EU's fundamental rights framework and strategic autonomy. However, by committing to broad cross-border data flows through DTAs, the EU risks undermining these two pillars of its data governance model: the voluntary, protected sharing promoted by the Data Governance Act, and the controlled, rights-based mandatory sharing framework established by the Data Act. Trade commitments prioritising data liberalisation without equivalent rights safeguards could severely weaken the effectiveness of both laws.

Last but not least, provisions in DTAs that prioritise cross-border data flows not only can undermine the EU's commitment to upholding fundamental rights but moreover, by facilitating ever-expanding data extraction and intensive computational infrastructures, **DTAs can run counter to the EU's Green Agend**a, entrenching environmentally harmful business models and obstructing regulatory efforts aimed at curbing the ecological footprint of the digital economy.

Acronyms

- AI Act: Artificial Intelligence Act
- DGA: Data Governance Act
- DMA: Digital Markets Agreement
- DSA: Digital Services Agreement
- DTA: Digital Trade Agreement
- EDPS: European Data Protection Supervisor

- EU: European Union
- EUSFTA: EU-Singapore Free Trade Agreement
- FTA: Free Trade Agreement
- GATS: General Agreement on Trade in Services
- GATT: General Agreement on Trade and Tariffs
- GDPR: General Data Protection Regulation
- WTO: World Trade Organisation

Annex: In-Depth Analysis of the Key Issues in the EU-Singapore DTA

The EU-Singapore DTA is designed to complement the EU-Singapore Free Trade Agreement (EUSFTA), which entered into force in November 2019, liberalising and enhancing bilateral trade relations between the EU and Singapore[4]. The EUSFTA was widely criticised for its incompatibility with EU data protection laws and its prioritisation of corporate interests over robust safeguards. The text of the DTA, authorised by the Council of the EU in April 2023 was concluded on 25th July 2024 and, at the time of writing, will soon be referred to European Parliament and Council for ratification. This Annex provides a detailed examination of two sets of provisions within the DTA that raise significant concerns in relation to digital rights: those referred to Data Flows and that regarding Access to Source Code.

As the first stand-alone digital trade agreement negotiated by the EU, it sets a potentially troubling precedent for future trade deals. While aiming to enhance bilateral trade relations, the DTA introduces provisions that may undermine the EU's ability to enforce its digital laws and safeguard citizens' rights. This analysis highlights the most problematic aspects of the agreement, focusing on its implications for privacy, data protection, algorithmic transparency, and the broader implications for EU regulatory standards. However, this does not mean that other provisions do not also raise concerns.

As mentioned above, while the DTA includes exceptions in these two sets of provisions, these are not enough to guarantee the EU's regulatory autonomy. The true impact of such provisions often becomes clear only when disputes are brought before a dispute resolution mechanism, that often prioritise market considerations over fundamental rights. The right to regulate and enforce does not stem from trade agreements, even if DTAs acknowledge its relevance (Article 3 of the DTA with Singapore); instead, these agreements are designed to restrict that right. Therefore, while exceptions provide some protection, they cannot be relied upon as sufficient safeguards, and the removal -or thorough rearticulation- of these provisions is essential to ensure the EU's regulatory framework remains intact.

EDRi will provide specific analyses on the agreement with Korea, and potentially other future agreements, once it has access to the relevant texts.

[4] The DTA also builds on the EU-Singapore Investment Protection Agreement, as well as on the Digital Partnership and the Digital Trade Principles.

Source Code Prohibition

The **source code provision** (Article 11) in the EU-Singapore Digital Trade Agreement limits the Parties' ability to require the transfer of or access to source code from companies, except under narrowly defined circumstances. While the inclusion of exceptions represents an improvement compared to older trade agreements, serious risks remain for **fundamental rights protection**, **regulatory autonomy**, and the **effective enforcement of EU law**.

The provision allows regulatory, law enforcement, judicial or conformity assessment bodies to access source code where necessary to ensure compliance with laws pursuing **legitimate public policy objectives**. Importantly, the agreement includes a **non-exhaustive list** of areas like public security, health, public morals, online safety, cybersecurity, safe AI, and disinformation. This explicit list constitutes a positive step compared to earlier texts where such concepts were left undefined. However, even with this definition, the structural problems persist. Footnote 1 to Article 5.4 also states that these must be interpreted **'in an objective manner'**, without giving fundamental rights priority over trade liberalisation. In practice, this means regulators trying to access source code to check for **algorithmic discrimination, market manipulation**, or similar harms may face **legal challenges**. These goals could be seen as too political or economic to qualify under the agreement's scope. The **burden of justification** lies entirely on regulators. They must prove a direct link between the source code access and a legitimate objective. Even then, companies can argue their code contains **trade secrets**, demanding procedural guarantees or delaying access, creating **chilling effects** on enforcement.

Worse still, **the safeguard against unauthorised disclosure in the EU-Singapore Digital Trade Agreement is vague**. It does not define the **level of protection required**, nor does it guarantee that source code access will be governed exclusively by EU laws and standards. This is especially problematic in cases where software systems - not only AI, but any complex digital infrastructure - process special categories of personal data (so-called 'sensitive data') under the GDPR. Without clear guarantees, regulators may be blocked from inspecting how this data is used, even when it is essential for enforcing compliance with fundamental rights. The lack of precision around how safeguards apply could severely limit authorities' ability to investigate or challenge harmful practices. This risks undermining the enforcement of EU rules on human rights, and could allow powerful firms to use procedural ambiguity, backed in this case by Singapore, to resist scrutiny.

Another major concern is the **exclusion of civil society and independent actors**. In principle, only public authorities - or those with formally delegated powers, a status that very few non-governmental organisations can obtain - are allowed to request access. This risks shutting out researchers, independent auditors, and civil society organisations, who often play a critical role in uncovering algorithmic and software-related harms. The result is a model of closed enforcement, with limited space for democratic oversight or independent accountability..

Competition enforcement is also at risk. Authorities can, in principle, demand source code to tackle digital market abuses, but only if the request is **proportionate, targeted**, and consistent with the agreement. Firms may argue that broad access to complex algorithmic systems is excessive. This risks obstructing scrutiny of **self-preferencing, algorithmic collusion, exclusion**, and other structural abuses.

Finally, the source code provision is supplemented by a **cross-reference to Article 9.3 of the Government Procurement Chapter of the EUSFTA, allowing additional exceptions** for protecting public morals, public order, public security, health, or essential security interests, which in principle could be a positive step. Yet this does not fundamentally alter the structural imbalance: regulatory measures invoking these grounds must still meet strict tests, and remain vulnerable to restrictive interpretations by dispute settlement bodies..

It is important to recognise that, as has been flagged throughout this analysis, DTAs could **seriously restrict future policy space**. The requirement to justify any access to source code under narrowly framed, high-burden exceptions could limit the EU's ability to respond flexibly to emerging challenges. As software-based solutions, particularly when it comes to AI, continue to evolve, affecting new sectors, uses, and forms of harm, the legal straightjacket imposed by this agreement could **prevent the timely development of new regulatory tools** necessary to protect fundamental rights, public welfare, and democratic oversight in a rapidly digitising society. And, as we have seen in the case of the AI Act, there are precedents.

Data Flows Provisions

As emphasised by the EDPS' Opinion 4/2025, **the DTA's provisions on free data flows have the potential to undermine the EU's domestic regulatory framework and weaken the protections offered by the GDPR and other critical pieces of legislation.** Furthermore, we are

afraid that while adequacy decisions and other Chapter V GDPR mechanisms can promote regulatory convergence, DTAs might instead lead to a ‘race to the bottom’ scenario, where weaker standards are adopted to facilitate trade, rather than ensuring robust protection for personal data.

The main limitations of the carve-outs in these provisions are explained in ‘Why Exceptions Don’t Work’, where it’s clear they might offer little legal certainty when rights protections come into tension with trade interests. The narrowness or vagueness of current carve-outs exacerbates the risk of regulatory capture or the weakening of data protection standards under the guise of trade facilitation.

- In this regard, Article 5(4) allows in principle a party to restrict data flows to achieve a legitimate public policy objective, which in principle could be positive, but sets an exceptionally high threshold:
  - Any measure aimed at restricting data flows must satisfy two criteria: it must pursue a 'legitimate public policy objective' and be 'proportionate' to that objective. It is thus subject to a subject to a full necessity test. As mentioned above, the poor track record of 'public policy' exceptions under GATT and GATS - with only 2 out of 48 cases upheld - raises doubts about their effectiveness in protecting fundamental rights in trade contexts.
  - The **combination of high evidentiary thresholds and the risk of legal challenges may have a chilling effect on regulators**, discouraging them from enacting measures that could be perceived as inconsistent with trade obligations. This dynamic risks creating a regulatory environment where commercial interests are prioritised over the protection of fundamental rights.
  - This provision is dangerous for the Data Act and, more broadly, for EU data governance for several reasons:
    - It could **undermine the EU's ability to impose necessary conditions on data transfers**. Yet, the Data Act relies on certain safeguard measures, particularly for sensitive public-sector data, data held by critical infrastructure providers, and potentially non-personal data where important public interests are at stake (e.g., cybersecurity, law enforcement access, industrial competitiveness). This trade rule would severely constrain the EU’s ability to impose or even adjust those requirements as new risks emerge.
    - It promotes a **presumption that data flows must always be free, unless narrowly justified otherwise.** The provision fosters the idea that cross-border data flows are the default and any restriction must be an exception - reinforcing a 'data

liberalisation first' logic. However, the Data Act is built precisely to create a balanced framework, ensuring that data use and sharing serve the public good, fundamental rights, and strategic autonomy. Free data flows without meaningful regulatory oversight would hollow out the Data Act's objectives.

- The push by EU Member States to establish a 'sovereign cloud'- particularly for critical sectors such as health, finance, and defence -highlights the **tension between the EU's strategic autonomy agenda and the legal constraints embedded in its trade agreements**. Article 5.4 of the agreement prohibits requirements for local data storage or computing infrastructure as a condition for doing business, except under limited and narrowly interpreted exceptions. This commitment could directly undermine efforts to mandate that sensitive data be stored and processed exclusively within EU-certified and EU-controlled cloud infrastructure. Moreover, by framing sovereignty not just as data localisation but as the ability of public administrations to control, switch, and negotiate with cloud providers, Member States are articulating a broader vision of infrastructural independence - one that risks being curtailed by existing trade obligations designed to prevent such differentiation. In practice, this raises serious concerns about the EU's ability to future-proof its digital infrastructure governance against foreign dependencies without breaching its own trade commitments.
- Similarly to the Source Code provision, it could **freeze regulatory space just when flexibility is most needed**. Digital technologies and risks evolve quickly (e.g., with AI, quantum computing, cybersecurity threats). The Data Act tries to anticipate some of this by enabling sector-specific rules and further safeguarding public interests. In contrast, this provision could lock the EU into commitments that are hard to amend later without risking trade retaliation or litigation, even if new risks or strategic needs arise. The vague promise of a review after three years offers no real flexibility.
- It risks undermining GDPR and fundamental rights protections as well. Although this provision refers primarily to 'data' generally (including non-personal data), the Data Act interacts with the GDPR and fundamental rights protections. For example, **where datasets mix personal and non-personal information and when data could be re-identifiable, restrictions are sometimes needed to protect data subjects' rights.** If measures safeguarding personal data flows are considered 'restrictions', this could invite challenges to GDPR adequacy

mechanisms, Standard Contractual Clauses, and other necessary safeguards.

It's critical to emphasise again that **the inclusion of data protection-related clauses in DTAs is theoretically intended solely as a defensive measure to protect the EU's ability to maintain its data protection framework without facing trade law challenges.** The free flow of personal data should continue to be governed exclusively by the instruments of the GDPR and LED (adequacy decisions, SCCs, BCRs, etc.), and trade agreements should not create new transfer mechanisms. **However, despite this important and welcome intention, there remain structural risks.** Embedding data protection language in binding trade agreements, even defensively, may contribute to longer-term pressures on the framing of data protection and privacy rules, both politically and legally. Concepts such as 'general application' could be subject to different interpretations, and the cumulative normalisation of data protection within a trade facilitation logic could ultimately affect the EU's regulatory autonomy and the full protection of fundamental rights.

Article 6, focused on personal data, appears on its surface to promote data protection; however, it is insufficient in several key ways, more notably compared to the 2018 horizontal clauses adopted by the European Commission:

- The **provision does not establish that Singapore 'recognises the protection of personal data' as a fundamental right.** Moreover, it fails to specify the required level or quality of data protection, leaving room for broad and potentially inadequate interpretations. As a result, Singapore could claim compliance by implementing only minimal safeguards, which may fall well short of EU data protection standards, such as the GDPR.
- Notably, given Singapore's specific regulatory context (see below), critical parts the provision, notably 6.2 that directly influences the scope of 6.11, **refer solely to the protection of personal data and not to privacy**. This is not a technical detail: in EU law, privacy and data protection are separate but equally fundamental rights. By omitting privacy in the operative parts of the agreement, the text risks aligning more closely with Singapore's narrower legal framework, which lacks constitutional privacy protections and permits wide exceptions to consent. In practice, this could limit the EU's ability to challenge data practices that infringe on privacy but not strictly on data protection, weakening regulatory enforcement and exposing people to harms the GDPR is designed to prevent.

- The provision additionally **does not include mechanisms to assess or enforce the adequacy of the legal frameworks adopted by the Parties**. Without independent oversight or accountability measures, there is no assurance that the stated protections will be meaningful or effectively implemented. There is no safeguard to prevent Parties from lowering their existing data protection standards to meet other trade-related obligations. In practice, this could create a potential 'race to the bottom' dynamic, where strong protections are perceived as trade barriers, Parties may feel incentivised to weaken them in order to attract investment, facilitate data flows, or avoid disputes. Without explicit guarantees that data protection will not be subordinated to commercial interests, trade commitments risk gradually eroding rights under the guise of regulatory 'coherence' or 'modernisation'.
- Additionally, as mentioned hereabove, the 2018 horizontal clauses introduced a positive right, stating that '*Each party may adopt and maintain the safeguards 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'.* However, **this provision has been weakened in the current DTA text**.
    - In close connection to this, the EDPS also pointed to the 2018 horizontal clauses as a benchmark when criticising the removal of the sentence: '*[N]othing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards*'. This clause was designed to ensure that, in the event of a trade dispute, the EU would not have to justify its data protection laws under the strict trade-related tests set out in the GATS. Without this explicit safeguard, there is a risk that EU data protection measures could be subjected to legal challenges, potentially forcing the EU to defend its data protection framework within a trade law context that may not fully account for data protection as a fundamental right.
    - The fact that the provision states that nothing in the agreement shall prevent a Party from adopting or maintaining measures it deems '*appropriate'* could create a broad and imprecise exception. While the flexibility might appear useful, it could ultimately undermine the core aim of protecting personal data. On paper, this clause could allow the EU to rely on the GDPR as a safeguard. But in practice, it might discourage Data Protection Authorities from enforcing rights robustly, for fear of overstepping what is seen as 'appropriate' under the agreement.

- Moreover, the EDPS, in its assessment of the Protocol amending the Agreement between the European Union and Japan for an Economic Partnership regarding free flow of data, had already highlighted the weakness of the wording of the clause starting with '*Nothing in this Agreement*' In particular, the EDPS raised concerns about the concept of '*conditions of general application*', as it remains unclear whether this would encompass all duly justified cases in which the EU might require specific controllers or processors to store certain personal data within the EU. This ambiguity could fail to fully safeguard the EU's regulatory approach to personal data protection.
  - The problem lies in the ambiguity of the term 'conditions of general application' and whether this would allow the EU to impose specific requirements for data storage within the EU/EEA in certain situations. For example, the EU might want to require that specific types of personal data be stored within the EU/EEA to ensure adequate protection of individuals' privacy rights. However, it is unclear whether such specific, justified measures would be considered 'conditions of general application' under Article 6(11). This uncertainty creates a risk that the EU may not be able to fully exercise its regulatory authority in protecting personal data in line with its fundamental rights obligations, potentially undermining the EU's ability to regulate cross-border data transfers effectively.
  - While the clause appears to preserve the EU's ability to regulate cross-border data transfers, it does so only under the condition that such transfers are enabled by rules of 'general application'. This phrase is open to interpretation and may be used to argue that targeted or risk-based restrictions - such as a ban on transfers to countries lacking judicial oversight or subject to mass surveillance - are not permissible. Such measures, while fully lawful under the GDPR (e.g. Articles 46-49), could be challenged for not being sufficiently 'general'. This ambiguity introduces legal uncertainty and may deter the EU from adopting or enforcing more granular safeguards where these are most urgently needed.

- Last but not least, the earlier EUSFTA with Singapore includes an explicit data flow commitment regarding financial data, which Article DTA 41.2(a) states is superseded by the DTA. However, the EUSFTA also contains an implicit data flow commitment derived from market access and national treatment, as cross-border services inherently involve cross-border data flows. The DTA does not explicitly override

this implicit commitment, suggesting it may still be in effect. Additionally, the new safeguard clause in the DTA begins with '*Nothing in this Agreement,'* implying it does not affect obligations from other agreements like the EUSFTA. As a result, the DTA does not supersede the implicit data flow commitment from the earlier agreement, meaning this commitment remains in place but with a much weaker safeguard and outside the scope of the new safeguard.

A weak Data Protection and Privacy Framework

The inclusion of provisions in the EU-Singapore DTA that facilitate cross-border data flows, and the loopholes created by weak exceptions, is even more deeply concerning when **one of the parties in the agreement operates with much weaker data protection and privacy standards than the EU**, and this is the case given Singapore's approach to surveillance and commercial data practices.

In Singapore, privacy is not enshrined as a constitutional right. The Personal Data Protection (PDP) law also includes exemptions for the public sector, meaning that government data practices are not subject to the same scrutiny as those in the private sector. While Singapore follows a Rule of Law framework, it interprets state responsibility, citizen obligations, and business compliance through a distinct lens, as outlined in the Singapore 'Model Framework,' first introduced in 2019 and updated in 2020 (IMDA & PDPC 2020). This framework largely focuses on ensuring private sector compliance with best practices, informed by public sector principles. However, it does not ensure active engagement from data subjects in the compliance process or monitoring, particularly through trusted third parties like data stewards. As a result, data subjects - who are the ones most affected by data sharing - are not typically included in the governance or enforcement processes that directly impact their privacy and data rights. The Act offers them limited rights over their data: for instance, withdrawing consent does not guarantee deletion, and organisations can retain data under broadly defined business purposes.

Mass Surveillance and State Access to Data. One of the most alarming aspects of the DTA is the potential for facilitating cross-border data flows without sufficient safeguards against mass surveillance. Singapore's data protection framework does not apply to government agencies, meaning that state authorities can access and process personal data without the same protections required of private entities. Additionally, there seems to be no independent body overseeing state surveillance practices, and the judiciary in Singapore has limited power to challenge government actions, which means that individuals' data can be accessed without proper scrutiny or

accountability. The specifics of surveillance operations remain undisclosed, creating a climate of uncertainty and mistrust.

In such an environment, the DTA's promotion of free data flows could encourage increased surveillance and undermine efforts to protect individuals' and collective rights. This provision may allow businesses to access consumer data more easily, but it also facilitates a regulatory environment where state surveillance can be conducted with little oversight or transparency. Singapore's legal framework, such as the Computer Misuse Act and the Internal Security Act, enables authorities to access private communications and monitor online activity. Given that the DTA encourages easier access to consumer data for businesses, it could also lead to more intrusive government surveillance under the guise of national security or other concerns.

A further concern under the DTA is the legal framework that enables law enforcement in Singapore to demand decryption or access to personal data during investigations. Under the Criminal Procedure Code, law enforcement agencies have the authority to compel individuals and companies to decrypt data and provide access to personal information in the context of investigations. This provision risks eroding privacy protections by allowing authorities to demand private data from individuals and businesses, potentially without sufficient oversight or safeguards. This broad authority to access encrypted personal data places individuals at increased risk of privacy violations, especially when the data is transferred across borders as part of the DTA. In scenarios where businesses hold sensitive consumer data, the free flow of data could expose individuals' personal information to potential misuse by state authorities, especially in the context of investigations that may lack independent scrutiny or judicial oversight.

Identity Tracking and Centralisation of Personal Data. Singapore has created a system where citizens and residents must register their national ID (NRIC) numbers, which are often linked to various digital services. This creates a centralised system of identity tracking, where an individual's personal data, used to register everything an individual did across many aspects of life, is interconnected across various platforms and services. The national ID number is frequently used in many digital services, which raises the spectre of a surveillance-based society where the movements, behaviours, and activities of citizens and residents are closely monitored. The centralisation of personal data increases the risks of mass surveillance and the potential for misuse of this data by both private companies and state authorities. The

DTA’s provisions could inadvertently support this trend, facilitating data flows that further entrench surveillance practices.

Censorship and Self-Censorship. Human rights defenders, journalists, and activists in Singapore have reported instances of self-censorship due to fears of surveillance and the potential consequences of state scrutiny. The pervasive surveillance environment in Singapore creates a chilling effect on freedom of expression and press freedom. Journalists and activists, especially those critical of government policies or actions, face the possibility of being targeted through surveillance or legal action. The DTA could exacerbate these concerns by promoting the free flow of data across borders without addressing the risks of surveillance or censorship. In a society where government agencies can track personal data, monitor online activity, and exert control over public discourse, the ability for individuals to freely express their views is severely restricted. The DTA’s provisions could facilitate the movement of data that could be used by both the government and businesses to suppress dissent and silence critical voices.

Weak Enforcement and Lack of Oversight. Despite the establishment of the Personal Data Protection Commission (PDPC) in Singapore, enforcement of data protection laws remains weak. Critics argue that penalties and oversight mechanisms are insufficient to deter major corporations from violating data protection rights, particularly in cases involving large-scale data exploitation. Companies have been fined for repeat offences, yet the penalties remain too low to create meaningful deterrence, especially compared to the fines imposed under the GDPR. Even when organisations are aware of vulnerabilities, they are often not compelled to act unless a breach has already taken place.

In addition, Singapore's lack of an independent data protection authority further compromises the effectiveness of its regulatory framework, as seen during a past Global Privacy Assembly, in which Singapore was excluded for its insufficiently independent DPA independence. Without strong enforcement mechanisms, individuals may struggle to seek redress in the event of data misuse or violations of their rights. This weak enforcement framework, combined with the absence of independent oversight, leaves the door open for companies and public authorities to exploit regulatory loopholes, further exacerbating the risks to privacy and data protection.

Concerns About China’s Influence. In addition to the domestic issues, there are concerns about external interference, particularly from China. Singapore’s close economic and political ties with China raise the potential

for Chinese authorities to influence or access data hosted in Singapore, further complicating the privacy landscape. Given that many multinational tech companies with a presence in Singapore operate in China or have data-sharing agreements with Chinese entities, the risk of cross-border data transfers to jurisdictions with even weaker privacy safeguards becomes a real concern. The DTA could inadvertently support such data flows, facilitating access to sensitive personal data that could be exploited by foreign governments, including China. The absence of clear safeguards and the lack of a robust data protection and privacy framework in Singapore create the potential for individuals' data to be accessed and misused by foreign governments without rights-based frameworks for this access, undermining privacy rights and the security of sensitive information.

Commercial Surveillance and Data Exploitation. Singapore has emerged as a critical hub for multinational technology companies, which rely on extensive data collection and exploitation as integral components of their business models. Firms such as Shopee, Grab, Meta, Google, and AWS have established significant operations in Singapore, where they process vast quantities of consumer data to refine ad targeting and business strategies. This data is frequently transferred across borders, raising serious concerns about the adequacy of privacy protections. With Singapore's regulatory framework offering limited safeguards, there is a tangible risk that it could become a 'digital trade hub' - a 'laundering' ground for data - a place where sensitive information can be funnelled through, bypassing stronger privacy regulations elsewhere and exposing users to potential exploitation without adequate oversight or accountability.

As mentioned in this document's introduction, while this Annex focuses primarily on the implications of the EU-Singapore DTA for EU digital regulation, it is important to emphasise that the effects of the agreement extend well beyond the EU legal order. The provisions at stake will also influence the digital rights landscape in Singapore, potentially shaping regulatory trajectories, access to rights, and the balance of power between public institutions, corporations, and individuals and communities inside and outside the country. Although we have not yet been able to engage directly with local communities and civil society actors in Singapore, their perspectives are essential to understanding how such agreements may reinforce or challenge existing inequalities, surveillance practices, and corporate dominance. A complete assessment of the DTA's impact must therefore include the lived realities and structural conditions in Singapore, and consider how digital trade commitments may constrain or enable rights protections in both jurisdictions.