Key points for consumers

EU-SINGAPORE DIGITAL TRADE AGREEMENT

More risks than benefits for consumers

BEUC The European Consumer Organisation

The Consumer Voice in Europe

Why it matters to consumers

EU consumers frequently shop online, but when buying from non-EU sellers they are exposed to risks such as unsafe products and unfair AI systems for consumer use. The Digital Trade Agreement between the EU and Singapore seeks to enhance consumer trust and confidence in the digital marketplace by improving access to information, safety and redress mechanisms, while providing businesses with predictability and legal certainty. However, certain provisions in the deal could weaken fundamental rights to privacy and personal data protection for EU citizens. Moreover, they risk limiting the EU's ability to enforce its digital laws domestically, such as the AI Act. If left unaddressed, these shortcomings could create risks for consumers.

On 25 July 2024, the EU and Singapore concluded negotiations on a Digital Trade Agreement, the first of its kind. Never before has a trade agreement focused solely on digital trade, but this new deal reflects the EU's ambition to become the global standard-setter for digital trade rules and cross-border data flows. The agreement includes binding rules to facilitate digital trade in goods and services between the two parties, including provisions on data flows, personal data protection, source code, online consumer protection, and spam. Some of these rules could enhance consumer trust online. Unfortunately, other elements fall short of established EU standards and could negatively impact the ability of the EU to enforce its digital laws. The consumer movement therefore cannot support the agreement in its current form.

This paper summarises BEUC's position on the negotiated deal with Singapore. The table assesses the proposals with the following symbols, illustrating whether BEUC:

 what BEUC supports

 what can be improved

 what is missing

COMMISSION PROPOSAL	BEUC POSITION
ARTIFICIAL INTELLIGENCE: ACCESS TO SOURCE CODE 	Foreign countries sometimes ask EU companies to provide access to their software source code to obtain a licence to operate in their markets. This tends to lead to intellectual property theft. To better protect companies, the EU agreed with Singapore to ban this practice in this agreement. We're concerned that the way this provision has been drafted may limit regulatory bodies' ability to ensure that companies comply with laws such as the AI Act. Without easy access to source code, investigations into fraudulent practices and security vulnerabilities could be obstructed, compromising consumer safety and trust. Companies already have protections for their intellectual property and trade secrets. This new layer of protection for companies could come at the expense of the enforcement of EU law and is therefore not proportionate to the intended goal.

COMMISSION PROPOSAL	BEUC POSITION
DATA FLOWS, DATA PROTECTION AND PRIVACY	This agreement changes the approach agreed in 2018 between the Parliament, the Council and the Commission on data flows. Indeed, the Commission is authorised to negotiate on data flows in trade agreements, provided that it won't impact its ability to preserve citizens' privacy and personal data. The current text does not fully comply with the said commitment. By adapting the EU model clause on data flows to the needs of Singapore, the Commission has brought legal uncertainty regarding the risk of a trade dispute over digital rights. Our concern is shared by the European Data Protection Supervisor, in relation to a similar deal with Japan. The Commission should have refrained from including this clause and instead negotiated an adequacy decision that would enable digital trade without compromising the EU's ability to pursue its policy objectives through regulation.
SPAM	The agreement provides important protections for consumers against unsolicited commercial electronic messages. It requires suppliers to obtain consent from recipients and offer clear options to opt out of further messages. The article also ensures transparency by mandating that commercial messages clearly identify the sender and provide information for recipients to stop communications. Additionally, provisions are included for cooperation between parties to regulate unsolicited messages and ensure access to redress for non-compliance. Despite this, we believe that the article could further expand the definition of spam to encompass not just messages, but communication in general. This would make the provision future-proof against emerging technologies, while also addressing the existing issue of telemarketing calls.
RIGHT TO REGULATE	It is encouraging to see key issues such as consumer protection, safety, environmental preservation, and privacy and data protection recognised as legitimate policy objectives. However, we are concerned about the ambiguity surrounding the notion of 'legitimate policy objective,' particularly regarding its potential legal implications within World Trade Organisation (WTO) frameworks. Historically, similar provisions, such as the GATS and GATT general exceptions[1], have been interpreted in ways that limit governments' ability to enact public policy measures aimed at protecting consumers, preserving the environment, and addressing other critical issues. This restrictive interpretation often arises from the WTO panel's strict application of the necessity test, which assesses whether such measures are essential and if less restrictive alternatives are available. Consequently, the threshold to prove compliance with these exceptions has proven extremely difficult to meet, resulting in only two successful applications out of nearly 48 cases.
ONLINE CONSUMER PROTECTION	In this deal, the EU and Singapore agreed to have protections in place to prevent traders from manipulating consumers online. Key provisions guarantee consumer rights to information and safety. Moreover, both sides agreed to ban misleading, fraudulent, and deceptive practices. This could protect buyers from false claims or undisclosed information. The deal also guarantees that consumers can act and claim their rights if something goes wrong after buying from Singapore traders online. This set of rules could empower consumers to make informed choices and be better protected online.

Avoid setting the wrong precedent

For upcoming agreements, such as Digital Trade Agreements with Korea, Thailand and the Philippines, BEUC urges the Commission to focus on benefits to consumers such as online consumer trust and safe payments, and refrain from including risky clauses on source code and data flows. On the one hand, more appropriate international forums than trade agreements should be used to address intellectual property theft, such as cooperation agreements. On the other hand, the EU has existing tools, such as adequacy decisions, to make cross-border data flows easier and safer.

[1] The General Agreement on Trade in Services (GATS), specifically Article XIV; General Agreement on Tariffs and Trade (GATT), specifically Article XX

BEUC The European Consumer Organisation

February 2025
BEUC-X-2025-015