BEUC The European Consumer Organisation

The Consumer Voice in Europe

Position paper

Digital trade rules that work for consumers



November 2026

Why it matters to consumers

Every day, EU consumers shop online and use digital services. As of 2026, over 80% of these services were provided by non-EU companies. This habit exposes consumers to a range of risks, such as spam or insecure payment methods. The EU's move to address this issue via digital trade rules is a positive step. However, the long-term implications of some of these rules remain uncertain and could undermine consumer welfare and trust in the globalised digital economy.

Published | 9 November 2026
Contact | international@beuc.eu
Reference | BEUC-X-2026-100
Document coordinator | Mykyta Sobko
Credit | Photo by Thirdman from Pexels

The European Consumer Organisation (BEUC) is the largest organisation promoting the general interests of Europe's consumers. Founded in 1962, it proudly represents more than 42 independent national consumer organisations from over 31 European countries. Together with our members, we inform EU policies to improve people's lives in a sustainable and fair economy and society.

BEUC, The European Consumer Organisation
Bureau Européen des Unions de Consommateurs, AISBL | Der Europäische Verbraucherverband
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.beuc.eu
Enterprise No.: BE 0422 071 051 • EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EISMEA. Neither the European Union nor the granting authority can be held responsible for them.

TABLE OF CONTENTS

1. Introduction 7
2. Core principles for digital trade policy to deliver to consumers 8
   - #1 Put consumers at the center 8
   - #2 Reinforce consumer trust online 8
   - #3 Preserve the EU's ability to regulate and enforce its laws 8
   - #4 Ensure transparency and meaningful civil society participation 9
3. Consumer protection in digital trade 9
4. Cross-border data flows and data protection 10
5. Algorithmic accountability and AI 12
6. Cybersecurity 13
7. Safe electronic payments 14
8. Enforcement and regulatory cooperation 15

Summary

Digital trade increasingly shapes how consumers shop, access services and interact online. As the European Union expands its network of digital trade agreements and incorporates digital trade rules into free trade agreements, it has an opportunity to ensure that these rules deliver tangible benefits for consumers.

Digital trade can promote innovation, choice and transparency. However, it can also expose consumers to risks, such as unfair commercial practices, inadequate data protection and cybersecurity vulnerabilities. To build consumer trust, **digital trade rules must support high levels of consumer protection and effective enforcement**.

This position paper sets out BEUC's vision for **a consumer-centred approach to digital trade**. The EU should ensure that digital trade rules preserve its ability to regulate in the public interest and uphold fundamental rights such as data protection. They should also promote accountability in emerging technologies, strengthen cybersecurity and support safe and affordable digital payments. **Digital trade policy should not only facilitate cross-border trade but also strengthen consumer protections** to develop a digital economy in a fair, secure and trustworthy way.

BEUC RECOMMENDATIONS

Put consumers at the heart of digital trade policy

1 Design digital trade rules to deliver tangible benefits for consumers, strengthen consumer rights and build trust online, with meaningful participation from consumer organisations and civil society.

Guarantee strong consumer protection online

2 Systematically include binding online consumer protection provisions in digital trade rules to secure a high level of consumer protection, effective redress and greater cooperation on consumer rights across jurisdictions.

Protect people's personal data and privacy

3 Ensure digital trade rules fully respect the GDPR and rely on the adequacy principle for international data transfers, and, if not, on contractual clauses and certification schemes. Any trade rules on data flows should fully reflect the EU model clause on personal data protection without alterations.

Avoid rules limiting access to source code

4 Preserve the ability of competent authorities and other legitimate entities to easily access source code or other relevant technical information to enforce EU law, assess compliance or conduct research.

Make digital products and services secure by default and by design

5 Instead of relying on companies to police themselves, digital trade rules should promote high mandatory cybersecurity standards so that products and services are designed to be secure from day one and come with safe default settings.

Deliver safe and affordable digital payments

6 Support the development of easily accessible, secure, affordable and transparent payment systems, while promoting international cooperation on fraud prevention and detection. Digital trade rules should also support greater transparency on payment costs and practices that reduce unnecessary fees for consumers.

Strengthen cross-border enforcement cooperation

7 Prioritise regulatory cooperation alongside digital trade rules to support cross-border enforcement, information sharing and coordinated responses to emerging digital challenges.

1. Introduction

Digital trade[1] has become central to consumers' daily lives. 94% of Europeans are online and most believe that digitalisation has improved their lives. Meanwhile, digital trade has grown into a multi-trillion-dollar component of the global economy. With more than half of the EU's trade in services now delivered digitally, the European Union has set itself the ambition of becoming a global standard-setter for digital trade rules.

Digital trade can deliver important benefits for consumers. It can promote innovation, expand choice, increase competition and make digital services more accessible across borders. However, it can also expose consumers to risks, including unsafe products, unfair commercial practices, misuse of personal data, fraud and cybersecurity threats. Whether digital trade ultimately works for consumers depends on the rules that govern it.

To shape these rules, the EU has progressively incorporated digital trade provisions into its free trade agreements and has begun concluding standalone digital trade agreements. These rules cover a wide range of issues that matter to consumers, including cross-border data flows, online consumer protection, electronic payments, cybersecurity and artificial intelligence.

Trade agreements do more than facilitate cross-border commerce. They create legally binding rules that continue to apply long after negotiations have ended. Once concluded, these rules shape how governments regulate markets and design future legislation. Any new EU or national measures must be compatible with the rules contained in the agreement, or risk being challenged by trading partners through international dispute settlement procedures. In practice, this means that digital trade rules adopted today can influence the consumer protection laws adopted tomorrow.

As the EU expands its digital trade agenda, EU digital trade rules should uphold the EU consumer acquis. It should also safeguard the Union's ability to regulate in the public interest. Digital trade should support, rather than constrain, future efforts to protect consumers in an evolving digital economy.

This paper sets out BEUC's vision for a consumer-centred digital trade policy and identifies the safeguards needed to make sure that digital trade rules work for consumers.

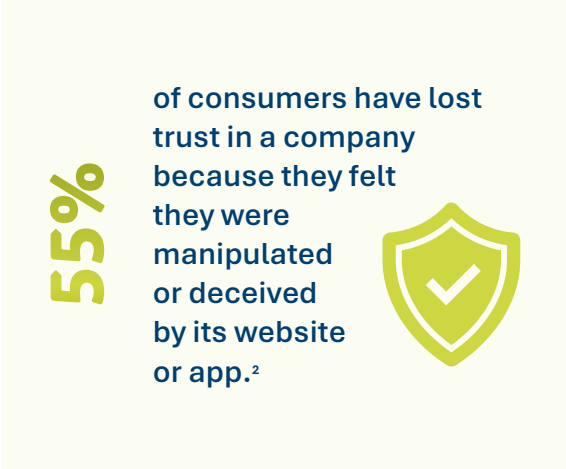
[1] Commerce enabled by electronic means

2. Core principles for digital trade policy to deliver to consumers

#1 Put consumers at the center

Digital trade agreements are often designed primarily through their economic impact on businesses. However, they should also be evaluated against their effect on consumers. Starting with an impact assessment carried out by the European Commission, policymakers should systematically assess whether digital trade rules improve consumer choice, strengthen rights and redress mechanisms, enhance transparency and privacy, and promote a safe and fair digital economy. This task should be required by the negotiating directive set by the Council.

#2 Reinforce consumer trust online



Consumer trust is essential for the growth of digital trade. Consumers must be confident that their rights are protected, that harmful practices are addressed and that effective remedies are available when problems occur. Consumers should be protected online, just like they are protected offline. Consumer protection should therefore be viewed not as a barrier to trade, but as a foundation of a well-functioning digital economy. The EU should use its digital trade agenda to reinforce the trust that digital markets currently struggle to maintain.

#3 Preserve the EU's ability to regulate and enforce its laws

Digital trade rules should strike a balance between facilitating cross-border digital commerce and preserving governments' ability to address legitimate public policy concerns. Digital technologies continue to evolve rapidly. Policymakers therefore need sufficient flexibility to respond to new challenges and adopt measures related to consumer protection, safety, sustainability, privacy and data protection.

The digital rules included in trade agreements can, however, affect the EU's ability to regulate and enforce its laws in the public interest. While trade deals increasingly recognise governments' ability to pursue legitimate public policy objectives, their legal

[2] BEUC, *Consumer survey results on the fairness of the online environment*, 2023

implications remain uncertain. Past WTO disputes offer an important lesson in this regard. They show that, even where trade rules provide exceptions for public policy objectives, it can be difficult in practice for governments to justify measures taken in the public interest. This means that recognising public policy objectives in an agreement does not necessarily guarantee governments their right to regulate.[3]

The EU should therefore ensure that its digital trade rules preserve sufficient regulatory space to maintain existing protections and develop future policies in response to technological and societal developments.

#4 Ensure transparency and meaningful civil society participation

Digital trade negotiations have far-reaching implications for consumers and society as a whole. Ensuring transparency and meaningful stakeholder engagement is therefore paramount to build trust in the process and guarantee that negotiating positions reflect a broad range of interests.

Meaningful participation requires more than being informed once negotiations are concluded. Consumer organisations and civil society should have timely access to information and opportunities to provide input throughout the negotiation process, allowing their expertise to help develop balanced and future-proof digital trade rules.

The EU has developed mechanisms to increase transparency and stakeholder input in trade negotiations. Through the Trade Civil Society Dialogue, the European Commission has provided stakeholders with opportunities to follow negotiations and exchange views. In the past, expert groups on EU trade agreements allowed civil society to contribute expertise to transparent and inclusive trade policymaking during negotiating rounds.

A step further would be for the European Commission to introduce a call for evidence or a public consultation on the substance of the negotiating directives before they are drafted. This would allow consumer groups and other stakeholders to provide evidence and input on the objectives of the future negotiations at the earliest stage of the process, in line with the Commission's broader Better Regulation and transparency principles.

3. Consumer protection in digital trade

Digital trade agreements should not only focus on facilitating cross-border commerce and reducing barriers for businesses. They should also ensure that the expansion of digital trade takes place in an environment where consumers are protected and able to exercise their rights.

[3] Centre for International Governance Innovation, As Global Trade Goes Digital, Trust Becomes Critical, 2023

69% **69% of 162 products from Shein and Temu (USB chargers, toys, jewellery) tested by Belgian, French, German, Dutch and Danish consumer groups failed to comply with EU safety rules.**



Consumers increasingly purchase goods and services online from businesses located abroad. Differences between national consumer protection frameworks can create uncertainty and make it more difficult for consumers to seek information, enforce their rights or obtain remedies.

> *In 2025, around **6 billion items** were released for free circulation, three times more than in 2022, largely driven by e-commerce from outside the EU.*[4]

Online consumer protection provisions in digital trade deals can help address these challenges. They can establish common obligations for traders, provide effective redress mechanisms and promote greater consistency in consumer protection rules across borders.

We therefore welcome the inclusion of binding online consumer protection provisions, such as provisions requiring clear information, prohibiting misleading, fraudulent and deceptive business practices, and promoting consumer safety. We also support the inclusion of redress mechanisms, which are essential to ensure that consumers can assert their rights and seek effective remedies when problems arise. These binding provisions should establish a common minimum level of consumer protection, while preserving the EU's and the partner country's ability to maintain or introduce stronger protections.

4. Cross-border data flows and data protection

The ability to transfer data across borders is one of the essential components of the digital economy. It allows consumers and businesses to access and provide digital services globally. Every day, consumers rely on cross-border data flows to send messages through apps, stream content, or access online services. However, when these flows involve personal data, facilitating transfers must go hand in hand with ensuring a high level of data protection and privacy to maintain consumer trust.[5]

[4] European Commission, *Report highlights need for stronger customs controls and cooperation to protect EU citizens and businesses*, 2026
[5] OECD Trade Policy Papers, *Trade and Cross-Border Data Flows*, 2019

> *In 2026, more than **8 in 10 Europeans** don't trust American or Chinese technology companies with their data.*[6]

The EU has developed a robust framework that allows personal data to move internationally while preserving a high level of protection for consumers. Under the General Data Protection Regulation (GDPR), personal data can flow freely to countries that provide an essentially equivalent level of protection to that guaranteed under EU law. This is achieved through adequacy decisions. Where no adequacy decision exists, businesses may rely on alternative safeguards, such as standard contractual clauses or approved certification mechanisms.

A key strength of the adequacy system is its flexibility. Because adequacy decisions are adopted unilaterally by the EU, they can be reviewed, suspended or withdrawn if developments in a third country reduce the level of protection afforded to personal data. This allows the EU to respond to political, legal or regulatory changes while maintaining a high level of consumer protection.

The EU should not include digital trade rules on cross-border data flows in its trade agreements that create parallel rules or weaken existing EU data protection safeguards. Facilitating data transfers without respecting the adequacy principle could expose consumers to risks by allowing their personal data to flow to jurisdictions where protections equivalent to those provided under EU law may not apply, increasing the risk of misuse.[7]

87% **of consumers consider it important to be able to trust a company with handling their personal data before using their services.**[8]



The EU should make sure that digital trade agreements fully preserve the GDPR framework and recognise data protection as a fundamental right. In line with the European Data Protection Supervisor's concerns, the Commission should apply the precautionary principle when negotiating cross-border data flow provisions, particularly when they concern personal data. Any provisions on cross-border data flows should fully respect the safeguards set out in the EU model clause on personal data protection and privacy. The EU should refrain from altering its meaning, as doing so could weaken protections for consumers and limit its ability to respond to future developments.

[6] Cluster17 and POLITICO, *European Pulse Survey*, 2026
[7] Digital Trade Alliance, *Data Transfer Rules as Geopolitics*, 2023
[8] BEUC, *The economic costs of weakening privacy and data protection*, 2026

5. Algorithmic accountability and AI

Software and AI systems are becoming increasingly sophisticated and embedded in the products and services consumers use every day. From online platforms and connected devices to recommendation systems and AI-powered tools, digital technologies are influencing consumers' choices, safety and access to services. As these systems become more complex, effective public oversight becomes increasingly important.

To protect consumers, authorities must be able to investigate how digital systems operate, verify compliance with the law and address potential harms. This may require access to technical information, including source code,[9] to determine whether products and services comply with rules on consumer protection, product safety, competition or artificial intelligence. Such access can also be necessary to detect discrimination, manipulation, safety risks and other harms to consumers and fundamental rights. Without such access, effective enforcement may become significantly more difficult.

At the same time, the EU is now including rules in its digital trade agreements that restrict access to source code, because it wants to protect companies' intellectual property and trade secrets. This is a legitimate objective, but it should not undermine the EU's ability to enforce its laws. Businesses already benefit from extensive safeguards under international and EU law, including the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights. Trade agreements should not create additional barriers that prevent authorities from carrying out their regulatory and enforcement duties.

> *Source code provisions in digital trade agreements may conflict with current and future Right to Repair legislation by preventing governments from requiring access to software or source code where this is necessary to give effect to repair obligations.*[10]

The implications of source code provisions extend beyond AI. A 2025 report commissioned by the Transatlantic Consumer Dialogue highlights that broad prohibitions on requiring access to or the transfer of source code could also undermine the implementation of Right to Repair legislation, where access to software embedded in products may be necessary to enable repairs. Although some exceptions are included in digital trade agreements to allow authorities to access source code, the default rule is non-disclosure. This makes authorities' work more complex and could constrain enforcement.

The EU should therefore preserve the ability of competent authorities and other legitimate entities, including researchers or consumer organisations, to easily access source code or other relevant technical information where necessary to enforce EU law,

[9] The human-readable instructions that define a system's behaviour, algorithms and models
[10] TACD, *Source Code: A Trade-Related Barrier to the Right to Repair*, 2025

assess compliance or conduct research. Trade rules should promote innovation and protect legitimate commercial interests without creating unnecessary barriers to accountability, independent scrutiny or future consumer protection measures.

6. Cybersecurity

In today's hyper-connected world, cyber threats from state and non-state actors do not stop at borders. A cyberattack or security incident in one country can affect consumers and businesses elsewhere. This is particularly true because digital products, services and infrastructure increasingly operate across borders. Embedding security by design and by default is therefore essential to prevent harm, protect consumers and ensure trust in digital markets.

60%

Phishing was the most common way cybercriminals gained access to their targets, accounting for around 60% of the cases identified by ENISA. This includes techniques such as phishing emails, phone scams, malicious spam and online advertising.[11]



The EU has the opportunity to lead global efforts on cybersecurity. Through initiatives such as the Cyber Resilience Act, the EU is establishing a new approach to ensuring that products with digital elements are secure by design and by default.

Digital trade rules can support international cooperation on cybersecurity, including through the exchange of information, cooperation between authorities and sharing of best practices. However, such rules should not promote self-regulation as a substitute for effective regulatory frameworks. Experience has shown that voluntary approaches alone have not been sufficient to ensure that connected products placed on the market provide adequate levels of security.

[11] European Union Agency for Cybersecurity, *ENISA Threat Landscape 2025*, 2025

7. Safe electronic payments

Electronic payments are an essential component of the digital economy, enabling consumers to purchase goods and services online and access cross-border digital services. As their use continues to grow,[12] digital trade rules should support payment systems that are easily accessible, secure, affordable and transparent.

22% **22% of adults and 18% of teens report being victims of a security breach or fraud related to a digital payment in the last five years.**[13]



The increasing use of digital payments has also increased consumers' exposure to fraud, scams, and cybersecurity risks. International cooperation can play an important role in addressing these challenges through information sharing, coordination between authorities and the exchange of best practices. Such cooperation should strengthen fraud prevention and detection while respecting data protection rules.

At the same time, consumers continue to face challenges linked to high payment costs, limited transparency and expensive dynamic currency conversion practices in cross-border transactions. Digital trade rules should promote transparent pricing and support payment solutions that help reduce costs for consumers while maintaining strong consumer protection safeguards.

> *If a new digital payment method was introduced, consumers say it should be secure and **reliable (55%), easy to use (53%), and with very low or no fees (49%)**.*[14]

Digital trade agreements should also accommodate public initiatives aimed at developing secure and innovative payment solutions. In the EU, initiatives such as the digital euro seek to strengthen payment resilience, foster innovation and provide consumers with an additional payment option. Future digital trade rules should not hinder such developments and should support interoperability between payment systems where it benefits consumers.

[12] European Central Bank, *Study on the Payment Attitudes of Consumers in the Euro Area (SPACE)*, 2024
[13] BEUC, *What Consumers Expect from the Digital Euro*, 2025
[14] BEUC, *What Consumers Expect from the Digital Euro*, 2025

8. Enforcement and regulatory cooperation

Binding digital trade rules can be difficult to adapt once in force. Given the rapid pace of technological change, regulatory cooperation can provide greater flexibility to respond to emerging technologies and consumer risks. In certain areas of digital trade, it should therefore be favoured over binding rules. Digital trade rules should go hand in hand with strong regulatory cooperation frameworks that allow authorities to address cross-border challenges while preserving their ability to adapt to future developments. Such cooperation should be voluntary and limited in scope, and should not replace legislative processes or limit the ability of authorities to take regulatory decisions.

In an increasingly globalised digital economy, effective consumer protection requires cooperation between national and regional authorities. Strengthening regulatory cooperation can help address cross-border harms while ensuring that public authorities have the necessary legal basis and tools to act effectively.

Existing mechanisms, such as the EU Digital Partnerships and Digital Dialogues, provide valuable platforms to deepen cooperation on areas including artificial intelligence, cybersecurity, digital infrastructure, data governance and emerging technologies. These frameworks should be further developed and expanded to support information sharing, exchange of best practices, coordination between regulators and, where appropriate, joint enforcement actions.

A good example of an area of cooperation that can deliver tangible benefits for consumers is telecommunications, particularly the removal of roaming charges.