

The Consumer Voice in Europe

EU PRINCIPLES FOR A FAIR, SAFE AND SUSTAINABLE DIGITAL SOCIETY



Contact: David Martin – digital@beuc.eu

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.twitter.com/beuc • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45



Co-funded by the European Union

Ref: BEUC-X-2021-120 - 22/12/2021

Summary

BEUC welcomes the Commission's initiative to develop a set of EU Digital Principles to promote and uphold EU values in the digital space as part of the [Digital Compass](#) to guide Europe's digital transformation by 2030.

This paper contains a series of suggestions from a consumer protection perspective to strengthen the draft principles put forward by the European Commission as part of the public consultation carried out between May and September 2021. The content of the paper reflects the input that BEUC submitted in response to this consultation.

BEUC comments on the draft EU Digital Principles

1. General comments

BEUC welcomes the Commission's initiative to develop a set of EU Digital Principles to promote and uphold EU values in the digital space, as part of its [Digital Compass](#) to guide Europe's digital transformation by 2030.

We call on the Commission, Council and Parliament to ensure that these principles, in their final form, do not become a mere display of political goodwill. They must bring real added value in terms of the protection of individual rights and freedoms, the protection of consumers and the creation of a fair, safe and sustainable digital society.

We call on the Commission, Council and Parliament to ensure a strong set of principles that guide the actions and vision of the European Union towards [a human-centric digital transformation](#), be it in applying existing laws and policies or the development and adoption of future policy initiatives and legislation. The principles should include a strong commitment to making EU legislation enforceable and ensuring it is effectively enforced which, so far, has been the Achilles heel of the protection of consumers and citizens in the digital world.

2. Comments on the specific principles

2.1. Universal access to internet services

Internet connectivity is essential for consumers to access digital products and services and to be able to live and work in the digital society. This includes not only ensuring strong fixed and mobile internet broadband connectivity but also high capacity wi-fi connectivity.

An open internet, which guarantees access and distribution of internet content and services without discrimination, is also a pre-condition for a healthy and fair digital economy and society. This must include not only ensuring net neutrality but also removing barriers that prevent consumers from accessing content within the EU. Geo-blocking is a form of discrimination when it comes to internet content access.

Finally, in addition to ensuring clear information about the terms and conditions applicable to connectivity services and the obligation to guarantee a high level of protection when using these services, it is important to also underline that the terms and conditions must be fair to consumers.

Considering the above, BEUC suggests the following changes, marked in bold and strikethrough, to strengthen the principles related to universal access to internet services:

- "Everyone should have access to the internet through an affordable, **high speed and high quality** ~~and adequate~~ connection."
- "Everyone should be able to access and distribute internet content and services without discrimination **or geo-blocking**."
- "Everyone should be clearly informed on the terms and conditions applicable to connectivity services available on the market, and benefit from a high level of protection when using them. **Terms and conditions must be fair. Information must be provided in a clear, succinct and easily understandable and accessible manner.**"

2.2. Universal digital education and skills for people to take an active part in society and in democratic processes

Digital skills and education are essential for consumers to be able to actively participate in the digital society, including access and enjoyment of digital goods and services. At the same time, no one should be left behind or treated unfavourably for not being able to use digital technology or for choosing not to make use of it. Therefore, the establishment of a right to remain 'offline' should also be considered.

It is also important to underline that while education and skills are an essential element, the frequent complexity of digital tools and unfair market conditions and behaviour by businesses cannot be compensated by increasing the skills and savviness of consumers.

Moreover, people can only understand technology such as AI if those who develop and make use of the technology explain its uses, risks and possibilities. Currently, it seems that the opposite is happening, AI is used to hide business practices. For example, consumers have no idea how their social media feeds are generated, why they see certain content or and how they are traced, profiled and targeted for advertising purposes. Consumers need more transparency obligations imposed on businesses and stronger prohibitions of harmful uses of AI¹.

Considering the above, BEUC suggests the following changes to strengthen the principles related to universal digital education and skills:

- "Everyone should have the possibility to acquire through education and training the necessary digital skills to take an active part in society, labour markets and in democratic processes, **and to enjoy all the benefits that the digital single market can offer. At the same time, no one should be left behind or treated unfavourably for not being able to use digital technology or choosing not to use it. Digital tools and services must be user friendly by design.**"
- "Everyone should be able to be empowered through education to navigate the digital (media) environment in a safe, critical and confident manner."
- "Everyone should receive safeguards for a healthy balance in their use of digital technologies for working, ~~and~~ learning **and accessing goods and services.**"
- "**Full transparency and** ~~An~~ understanding of technologies, such as Artificial Intelligence should be promoted, so that it is possible to engage critically and ethically with them in everyday life and exercise the respective rights.

2.3. Accessible and human-centric digital public services and administration

Everybody should be able to access public services and public administration. Public procurement can be an important driver of socially valuable innovation and public

¹ See "[Regulating AI to protect the Consumer](#)" BEUC, October 2021

administration must lead by example when it comes to the respect and promotion of European values.

Considering the above, we suggest including the following additional principle in this section:

- (...)
- **Public procurement must promote digital social innovation and technology for the common good, and invest only in digital tools and services that respect EU legislation as well as European fundamental rights and values.**

2.4. Access to digital health services

Health services are one of the areas where digitisation holds the biggest potential for consumers. It is also one of the areas where the risks are greatest, not only in terms of possible abuses and harms e.g. due to privacy breaches and cybersecurity incidents, but also in terms of exclusion.

The preference or possibility of not using a digital health product or service should be respected. For example, the right to go to the doctor in person must continue to exist.

Consumers must also have full control over their health data. They must have a right to decide how and with whom they share data and be able to access their medical records and report on errors. Digital health tools and services must particularly respect principles of privacy-by design and security-by-design.

Considering the above, we suggest the following additions to the principles included in this section:

- *"Everyone should have access to the full benefits of digitisation of health and care services, including personalised medicine and telemedicine."*
- *"Digital health and care services should be inclusive, accessible, equitable and designed to meet peoples' needs, **fully respecting the principles of privacy and security by design and by default.**"*
- *"Everyone should have secure, digital access to their electronic health records and **be able to report on any errors that such records may contain.**"*
- *"**To access essential healthcare services the use of digital tools and services should remain a choice for consumers, not an obligation.**"*

In addition, we would like to highlight that legal gaps exist both at national and EU level in relation to the safety of telehealth services. For instance, as regards healthcare professional's qualification in telemedicine, there must be a common definition of what constitutes a medical act and a common approach on liability of the cross-border telehealth services across the EU. The EU must close these gaps to enhance consumer safety.

For further information on BEUC's position and recommendations on digital health please see [this position paper](#).

2.5. An open, secure and trusted online environment

These principles are absolutely key from a consumer perspective, particularly taking into account the structural [digital asymmetry](#)² which consumers face in the online environment.

The fundamental asymmetries of power and information between businesses and consumers which characterise the digital environment disempower consumers and cause

² See "[EU consumer protection 2.0 : Structural Asymmetries in Digital Consumer Markets](#)", Natali Helberger, Orla Lynskey, Hans-W. Micklitz, Peter Rott, Marijn Sax and Joanna Strycharz – March 2021; and "[The Regulatory Gap: Consumer Protection in the Digital Economy](#)", Natali Helberger, Hans-W. Micklitz and Peter Rott – December 2021

them to be in a permanent state of vulnerability. Businesses have real-time influence on shaping the digital environment that consumers find themselves in. They can access consumers' detailed personal profiles, including decision-making biases and pressure points. Businesses can exploit consumers' behaviour and vulnerabilities in ways never seen before. This leaves consumers continuously exposed to privacy abuses and manipulation, and fundamentally threatens their autonomy and freedom of choice.

We propose the following changes to strengthen the principles in this section:

*"An open, **fair**, secure and trusted online environment"*

- *"Everyone should be able to enjoy an open, **fair** and transparent online environment, where a diversity of opinions is encouraged and protected, **there is a balance of power between businesses and consumers/citizens, and business models are respectful of individuals' rights and freedoms.**"*
- ***Everyone should be able to participate in the digital society and use digital technology without being subject to commercial surveillance, discrimination and manipulation.**"*
- ***"Everyone should be protected against the state of vulnerability stemming from the structural asymmetries of power between businesses and individuals in the digital environment."***
- *"Everyone should be able to enjoy a safe and trusted online environment, where ~~illegal content and goods~~ **activities** are effectively tackled, and should be **strongly** protected against cybercrime and/or attacks."*
- *"Everyone providing **or accessing** ~~their~~ services online, **including via online platforms**, should expect fair dealing, **healthy competition and the protection of consumer choice**, including in their relationship with ~~online platforms.~~"*
- *"Everyone should benefit from confidentiality of their electronic communications (e.g. phone conversation, emails, etc.) and **strong protection against unauthorised access or misuse of** ~~information on~~ their electronic devices (e.g. computers, phones, ...)."*

2.6. Protecting and empowering children and young people in the online space

The EU must provide children and young people with additional protections in the digital environment, particularly to protect them against the commercial surveillance and exploitation of their activities.

Children are among the most active and engaged users of digital products and services. They are exposed to screens and online content from a very early age and are particularly vulnerable to the dangers of the digital world (tracking, profiling and harmful marketing^{3 4}, privacy and cybersecurity risks^{5 6}, manipulation, dark patterns, addiction and other psychological illnesses such as depression, etc).

We suggest the following additions to strengthen the protection and empowerment of children and young people in the online space:

- *"The online environment should foster children's and young people's well-being and their participation as digital citizens."*

³ ["Food marketing to children needs rules with teeth"](#), BEUC – September 2021

⁴ ["TikTok Without Filters"](#), BEUC – February 2021

⁵ ["#Toyfail: An analysis of consumer and privacy issues in three internet-connected toys"](#), Norwegian Consumer Council – December 2016

⁶ ["Watchout: An analysis of smartwatches for children"](#), Norwegian Consumer Council – October 2017

- *"Children and young people should be equipped with digital literacy and the necessary skills and competences to navigate safely and responsibly online from an early age and throughout their education and training."*
- *"Every child should be protected from harmful and illegal content, including from child sexual abuse and exploitation."*
- ***"Children should be protected from any form of online or offline commercial surveillance, in particular they should not be tracked, profiled or targeted for commercial purposes on the basis of a digital record of their activities, or of their actual or inferred interests or characteristics, including through the use of group or collective data, targeting by association or affinity profiling."***
- ***"Children should be protected from exposure to digital marketing, in particular exposure to advertising or other commercial practices which are harmful for children's mental and physical health, hidden advertising and new forms of commercial communications often not recognisable to them, such as influencer marketing and gamified advertising"***.

2.7. A European digital identity

Most consumers' everyday activities already take place wholly or partly online, and this is only likely to increase. Having access to a secure and trustworthy digital identity is becoming more and more important for consumers to securely access public and private services in the online environment. On the other hand, consumers should not have to confirm their identity constantly.

We propose to add the following to the principle put forward in this section:

- *"Everyone should have access to a secure and trustworthy digital identity that can be used anywhere in the EU to access a broad range of public and private online services. **This digital identity must guarantee the highest levels of data protection, privacy and security and its use should only be required in appropriate and justified circumstances.**"*
- *"Everyone should be protected against identity theft, alteration or manipulation."*

2.8. Access to digital devices, systems and services that respect the climate and environment

There is no doubt that the digital and the [green transformations](#) must go hand in hand. Digital technology holds great potential to help to improve energy efficiency and address the environmental challenges we face. A majority of the respondents to a [survey](#) carried out by BEUC members in 9 EU countries⁷ thought that that AI will help to make the world more sustainable.

Digital tools are also particularly important to enable a critical mass of consumers to become flexible in their energy consumption ([demand side flexibility](#)). This flexibility is a crucial element not only for individual consumers so that they can manage their consumption, but also collectively for the overall sustainability of a more renewable-based energy system. If a critical mass of customers becomes flexible in when and how much they consume electricity, this should reduce pressure on the energy grid and lead not only to more efficiency but to reduce the need for new investments and lower maintenance costs, in turn reducing levies and taxes as well. Contracts that provide demand side flexibility should be fair and in particular provide transparent pricing conditions.

⁷ Test Achats/Test Aankoop – Belgium; Forbrugerrådet Tænk – Denmark; UFC-Que Choisir – France; vzbv – Germany; Altroconsumo – Italy; Federacja Konsumentow – Poland; Deco Proteste – Portugal; OCU – Spain and Sveriges Konsumenter – Sweden

On the other hand, digital technology can also act as a 'fire accelerant' in terms of energy consumption, exploitation of natural resources, carbon emissions and waste production.

We propose the following changes and additions to the principles proposed in this section:

- *"Everyone should have the possibility to obtain information on the environmental footprint **impact** of digital products and services."*
- *"Digital products and services should be produced, **transported, packaged, and used and disposed** of with the lowest possible environmental impact."*
- *"**Digital products and services must be built on sustainable business practices and consumers should be strongly protected against premature obsolescence. Devices must be durable and easy to repair and reuse and software updates should be provided to ensure devices can be used securely during their expected lifetime. Consumers should be able to buy, sell, rent and exchange second-hand digital goods**".*
- *"**Digital tools and services that contribute to the green energy transition, such as those that enable demand side flexibility, should be transparent, easily available, affordable and user friendly.**"*

We would like to highlight that, while we fully support the first principle, we strongly object to the Product Environmental Footprint (PEF) method.

2.9. Ethical principles for human-centric algorithms

AI products and services, such as virtual assistants and facial recognition tools, are already changing consumer markets and our societies. It is a technology which carries huge expectations of improving and making consumers' lives more convenient. But the use of AI also comes with great risks and has major implications for consumers' autonomy and self-determination, their privacy, their capacity to interact with products and services and, ultimately, in the ability to hold businesses responsible if something goes wrong. Consumers must have rights and protections to ensure that the development and use of AI technology respects the EU's fundamental rights and values. In this sense, it is particularly important to move beyond an "ethical" framing in favour of strong [legally binding rules and principles](#).

We propose the following changes in this section:

"~~Ethical~~ Principles for human centric algorithms"

- *"**Algorithmic systems should be fair, transparent, secure and non-discriminatory.**"*
- *"No one should be limited or ~~purposefully~~ misguided by algorithmic systems against their autonomy and free will."*
- *"Everyone should benefit from algorithmic systems that foster their individual and societal well-being."*
- *"**Everyone should have the possibility to contest and obtain human oversight of a decision taken by an algorithmic system which significantly affects them.**"*

2.10. An additional principle on access to justice

In addition to the new principles suggested above in the respective section, we suggest adding the following principle:

Access to justice in the online environment

"Everyone should have access to effective remedies and redress mechanisms, including collective redress, when their rights are not respected in the digital environment, regardless of where the service provider is located. Authorities must be equipped to fulfil their enforcement and control role effectively. Sanctions and remedies must be adapted to the specificities of digital markets and efficient EU wide enforcement must be ensured."



This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).

The content of this publication represents the views of the author only and it is his/her sole responsibility; it cannot be considered to reflect the views of the European Commission and/or the European Innovation Council and SMEs Executive Agency (EISMEA) or any other body of the European Union. The European Commission and the Agency do not accept any responsibility for use that may be made of the information it contains.