



CONSUMERPRO

BOOSTING PROFESSIONALS
IN CONSUMER PROTECTION

Digital Rights

Theoretical background document

2022- 2023

TABLE OF CONTENT

Table of content.....	2
Introduction to the Theoretical background document.....	4
1. Data Protection	5
1.1. Introduction and history of Data Protection consumer policy	5
1.2. Why Data Protection matters to consumers	5
1.3. Main challenges concerning Data Protection consumer policy.....	5
1.4. Key consumer rights and obligations in a nutshell	6
1.5. Laws and Regulations at EU and national level	7
1.6. Case law	7
1.7. What can consumers do if they have a problem?	7
1.8. Further resources – factsheets, publications, links	9
2. Platforms	10
2.1. Introduction and History of Platforms consumer policy.....	10
2.2. Why Platforms matter to consumers.....	11
2.3. Main challenges concerning Platforms	11
2.4. Key consumer rights and obligations in a nutshell	14
2.5. Outlook: The upcoming Digital Services Act	15
2.6. Laws and Regulations at EU level.....	16
2.7. Case law	17
2.8. What can consumers do if they have a problem?	17
2.9. Further resources – factsheets, publications, links	18
3. Internet of things (IOT).....	19
3.1. Introduction & History	19
3.2. Why IOT matter to consumers.....	19
3.3. Main challenges within IOT.....	19
3.4. Key consumer rights and obligations in a nutshell	20
3.5. Laws and regulations at EU level	21
3.6. Case law	22
3.7. What can consumers do if they have a problem?	22
3.8. Further resources – factsheets, publications, links	23
4. Annex - List of eCommerce directive CJEU case Law	Error! Bookmark not defined.



This material was produced in the context of the project [Consumer PRO](#), which is an initiative of the European Commission under the European Consumer Programme. The European Commission's support does not constitute endorsement of the content which reflects the views only of the authors. The Commission cannot be held responsible for any use which may be made of the information contained therein.



1. DATA PROTECTION

1.1. Introduction and history of Data Protection consumer policy

The protection of natural persons in relation to the processing of personal data is a fundamental right in the European Union. Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provides that everyone has the right to the protection of personal data concerning them. In addition, Article 7 of the Charter of Fundamental rights states that everyone has the right to respect for their private and family life, home and communications.

The General Data Protection Regulation (GDPR) is the law that regulates the processing of personal data in the EU. It requires organisations, both public bodies and companies, to use consumer's personal data in a transparent and fair manner. It strengthens your rights and applies to all organisations which process the personal data of individuals who are in the EU, irrespective of where the organisations are based.

The rules on ePrivacy (currently the ePrivacy Directive, which is under review) protect the confidentiality of electronic communications and also contain specific protections for consumers against unsolicited commercial communications sent via electronic communication services.

1.2. Why Data Protection matters to consumers

Although beneficial to consumers, digital information technologies and the emergence of **new online services also** represent a **major challenge to the fundamental rights of privacy and personal data protection**. The business models that currently dominate the digital world are based on tracking and analysing consumers' every move. Companies utilise the information they gather to build user profiles, which are traded online and used to deliver behaviourally targeted advertising. These profiles could also be used to discriminate consumers and influence their behaviour. It is important to ensure that consumers can remain in control of their personal data and benefit from innovative digital products and services without having to give up their privacy.



1.3. Main challenges concerning Data Protection consumer policy

It is very difficult for consumers to be able to control what happens with their data in practice. Their rights are very often not being respected and they are often forced to accept giving up their privacy if they want to use digital products and services.



Consumers are under constant commercial surveillance and their personal data is exploited by a myriad of companies, many of which they have never even heard of. Privacy policies are vague, long, complex and very hard to understand and the consumer has no choice but to agree. Consumers are often given an illusion of control and in those cases where they are asked for their consent, this becomes a systematic, meaningless “tick the box” exercise on the part of the consumer.

The GDPR was meant to address many of these issues. However, almost four years after it entered into application, there have been no significant changes in business practices. The level of compliance is low in certain areas and enforcement is for the moment not fully efficient. Data Protection Authorities are having difficulties to cope with all the complaints they are receiving and the new enforcement architecture, built around a cooperation and consistency mechanism to ensure the coherent interpretation and application of the law across the EU, is facing important challenges.

Another issue is that the reform of the ePrivacy rules, which are meant to complement the GDPR and further protect the confidentiality of communications, is pending since more than five years and still there is no agreement in sight. (For more info about the ePrivacy Regulation see [BEUC factsheet](#)).

1.4. Key consumer rights and obligations in a nutshell

The GDPR requires organisations, both public bodies and companies, to use consumers’ personal data in a transparent and fair manner. It contains a series of [principles that govern](#) the use of personal data:

It also gives consumers a [series of rights](#) to ensure they can be in control of their data. Among others, consumers have the right to:

- Be informed, in a clear and easy-to-understand manner, about how their personal data is being used. This must specify which data is used, by whom and for what purposes.
- Access the data that organisations hold about them and obtain a copy of the data.
- Rectify their data if it is inaccurate.
- Get organisations to delete their data.
- Ask organisations to stop using their data, either temporarily or permanently.
- Receive their data in a commonly used format, so they can take it and use it somewhere else.
- Contest automated decisions based on their personal data that affect them in a significant manner (e.g. being denied a loan).
- Be informed if their data is lost or stolen.



- Lodge a complaint with their national data protection authority or bring a company to court

1.5. Laws and Regulations at EU and national level

- [EU Charter of Fundamental Rights](#)
- [Regulation \(EU\) 2016/679](#) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR).
- [Directive 2002/58/EC](#) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) – Amended by [Directive 2009/136/EC](#)
- [Guidelines, recommendations and best practices from the European Data Protection Board](#)
- [Opinions from the European Data Protection Supervisor](#)
- [Example of Code of Conduct: Federation of Direct Marketing](#)

1.6. Case law

For a repository of Data Protection Authority and Court decisions, as well as articles about the GDPR, visit: www.GDPRHub.eu.

On the official EU Law Portal: [Eurlex](#) file on GDPR. This is a list of European Court of Justice cases and preliminary questions that relate to the GDPR: find the list of case law under “document information”.

1.7. What can consumers do if they have a problem?

If the consumer considers that their rights under the GDPR have been violated there are two options:

- Filing a complaint with the national data protection authority. You can find the full list [here](#).
- File an action directly in court against a company/organisation. This doesn't stop the consumer from lodging a complaint with the national Data Protection Authorities if they wish.

Also, if the consumer believes that the Data Protection Authorities has not handled their complaint correctly or if they are not satisfied with its reply or if it doesn't inform them with regard to the progress or outcome within 3 months from the day the complaint was lodged, the consumer can bring an action directly before a court against the DPA.



Public authorities

At national level:

The national ministries in charge of data protection (normally this would be the Ministry of Justice), which set the national policy on the topic and should ensure the implementation of the GDPR at national level.

In addition to the national Data Protection Authorities, other public bodies worth considering are:

At European Level:

- The European Commission, which is in charge of ensuring that Member States correctly implement the GDPR and also has the power to “activate” certain provisions of the GDPR via delegated acts (e.g. for the creation of standardised “privacy icons”).
- The [European Data Protection Board](#) (EDPB), which gathers all the national Data Protection Authorities. Its main task is to ensure the consistency in the application and interpretation of the GDPR.
- The [European Data Protection Supervisor](#) (EDPS), which oversees the respect of people’s personal data by the EU institutions and advises the Institutions on data protection matters.

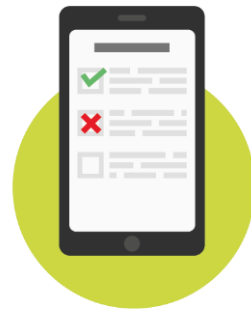
Alternative Dispute Resolution (ADR)

Out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to personal data processing can be established via codes of conduct adopted by industry bodies (Article 40 GDPR), without prejudice to the rights of data subjects to lodge complaints with their Data Protection Authority and to seek judicial remedies in Court.



1.8. Further resources – factsheets, publications, links

- [European Commission website with information about GDPR](#)
- [European Commission GDPR Library - Infographics, factsheets and other materials aimed at citizens and businesses](#)
- [BEUC Factsheet – What does EU data protection law mean to you?](#)
- [BEUC Report – The long and winding road: A cross border data protection enforcement case from a consumer perspective](#)
- [AccessNow – User guide to data protection in the EU: Your rights and how to exercise them](#)
- [Fundamental Rights Agency – European Data Protection Handbook](#)
- Guides published by Data Protection Authorities at national level (check the website of your national Data Protection Authority)
- [Factsheets](#) published by the European Data Protection Supervisor (EDPS)
- [The History of the GDPR](#) and a [Glossary](#) (EDPS)



2. PLATFORMS

2.1. Introduction and History of Platforms consumer policy

Consumers buy more and more services and products online, particularly through platforms.

In the early years of e-commerce such purchases took place mainly on websites of companies who also had brick-and-mortar shops on the high streets. Today, consumers' purchasing behaviour is radically changing: more and more people order services and products through online marketplaces which are shipped onto European consumers directly from outside the EU.

Purchases are not only made through e-commerce platforms such as Amazon Marketplace, AliExpress, wish.com or eBay but also through social media platforms such as Instagram.

For example, in 2017 approximately 100 million sales were dispatched from China to Germany. This is 40 million more than in 2016. Tremendous increases have also been reported in other European countries.

In addition, scams are on the rise with regards to web shops being set up in the EU by sellers pretending to be European companies but who are in reality ordering on platforms from China, and selling on these products to consumers for a higher price than for example on wish.com. This has been observed in Denmark and in France¹.



There are also very serious concerns that many of these products are not complying with European laws and technical standards which are in place to protect consumers' rights, safety, health and the environment². While manufacturers and distributors located in the EU can be held liable for product safety and compliance, this is often not the case for producers who are not located in the EU, as the intermediaries, i.e. the e-commerce platforms, deny responsibility for compliance.

There are important legislative initiatives currently under discussion to tackle some of these problems, notably the proposal for a Digital Services Act³ and the proposal for a General Product Safety Regulation.⁴

¹<http://www.leparisien.fr/economie/consommation/achats-en-ligne-attention-aux-derives-du-dropshipping-16-01-2020-8237226.php>

² <https://www.beuc.eu/publications/two-thirds-250-products-bought-online-marketplaces-fail-safety-tests-consumer-groups/html>

³https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021PC0346&from=EN>

2.2. Why Platforms matter to consumers

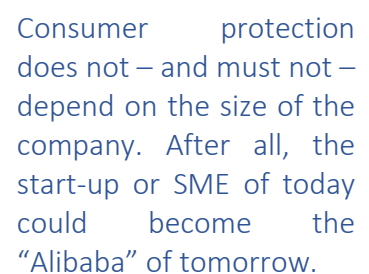
Shopping, connecting with friends and family, sharing experiences, watching a movie, listening to music, reading a book, booking a trip, cooking a new recipe, planning a night out, moving around a city, asking for your neighbours' help, and looking for information on the web; these are just some basic examples of activities that millions of consumers carry out every day. For each and every one of these activities, there is one or multiple online platforms that facilitate these services. Consumers have embraced the surge of the platform economy, which presents numerous benefits as well as challenges for consumer protection.

2.3. Main challenges concerning Platforms

Generally, when the eCommerce Directive was adopted (in 2000), platforms like Google, Amazon or Booking.com were in their infancies. Many other intermediaries did not even exist. For example, Facebook and Shopify were launched in 2004. Etsy was founded in 2005; Airbnb in 2008. Instagram, Wish and AliExpress saw the light in 2010.

Over the past 20 years, the business models of some of these and other companies changed. The market power dynamics have also changed.

The European digital market landscape has experienced “*datafication*” (the transfer of information into data, and this being the base of digital business models); a multiplication of platforms; a proliferation of the collaborative economy⁵; and a diversification of service providers in terms of functions, vertical integration and size. Yet, every single company has to play by the rules. Consumer protection does not – and must not – depend on the size of the company. After all, the start-up or SME of today could become the Alibaba of tomorrow.



Consumer protection does not – and must not – depend on the size of the company. After all, the start-up or SME of today could become the “Alibaba” of tomorrow.

Many platforms have reinvented themselves. Some no longer limit themselves to their initial role of information or trusted intermediaries (e.g. comparison or ranking platforms like Yelp) but enable transactions to be concluded on the platform. These are business models that make the platform fall under the category “*online marketplace*”⁶, which is the current focus of consumer protection organisations. This type of platform is defined under the Omnibus Directive⁷ as “*a service using software, including a website, part of a website or an application, operated by or on behalf of a trader which allows consumers to conclude distance contracts*”

⁵ http://www.beuc.eu/publications/beuc-x-2016-030_gbe_collaborative_economy_beuc_position.pdf

⁶ Vzbv study,

https://www.vzbv.de/sites/default/files/downloads/2020/02/12/vzbv_gutachten_verbraucherrechtliche_plattformhaftung.pdf, p. 17.

⁷ Article 2(1)(n) of the Unfair commercial practices Directive, as amended by Directive 2019/2161”, <https://eur-lex.europa.eu/eli/dir/2019/2161/oj>

with other traders or consumers”. Having said that, often the role of the platform is not limited to enabling the conclusion of a contract between sellers and buyers, but it also includes other services such as payment services, fulfilment services, returns processing and complaints handling⁸.



Other platforms have acquired multiple roles. There are “hybrid platforms”, which can combine different intermediary functions or vertically-integrated platforms. The latter do not only act as intermediaries, but also compete with traders, either directly or via affiliated companies. For example, Amazon is a seller, an online marketplace, a cloud computing company, a video-sharing platform, a publisher, an advertising company, a manufacturer of connected devices and an artificial intelligence company.

Consumer organisations advocate for adjustments in the legislative framework to address this new market reality. The proposal for a Digital Services Act (DSA) is a very important initiative in this perspective. The Commission put forward the DSA proposal in December 2020. It is currently in the final stages of the legislative process. An agreement is expected in 2022.

Specific challenges

Challenge #1. Spread of a wide range of illegal content.

Digital services have – to some extent – become an enabler for widespread consumer law violations; a revenue stream for the sale of advertising or promotion of dangerous, unsafe, illegal products online. For example⁹:

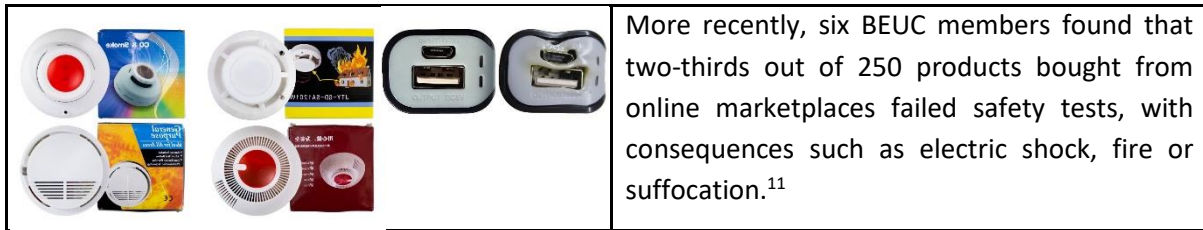
	<p>BEUC’s UK member Which? found Christmas tree lights sold online that could catch fire or electrocute consumers¹⁰.</p>
	<p>The Danish Consumer Council revealed cosmetics on wish.com not to comply with EU law</p>

⁸ Vzbv study,

https://www.vzbv.de/sites/default/files/downloads/2020/02/12/vzbv_gutachten_verbraucherrechtliche_plattformhaftung.pdf, p. 18.

⁹ See examples at https://www.beuc.eu/publications/beuc-x-2019-072_new_evidence_from_beuc_member_organisations_regarding_dangerous_products_available_online.pdf

¹⁰ <https://www.which.co.uk/news/2019/12/these-christmas-tree-lights-bought-online-at-ebay-wish-and-aliexpress-could-catch-fire-or-electrocute-you/>



Challenge #2. Confusion between online marketplace activities and other platform activities.

The debate to reform the e-Commerce Directive is to some extent focusing on issues like hate speech, terrorist content, copyrighted material, freedom of speech or single market considerations. While these are important issues, the EU should also not lose sight of specific consumer protection problems. It is necessary to ensure consumers who buy products or services through online marketplaces¹² are fully protected.

It is necessary to distinguish between the sale of illegal products and other activities, e.g. posting comments on social media. While in the latter case there are clear freedom of expression considerations, in the former case the main issue at stake is far from freedom of speech, but rather a product safety and a consumer protection issue.

Challenge #3. The eCommerce Directive does “*not apply to service providers established in a third country*”¹³.

Some providers established in third countries are exploiting the territoriality limitations of the Directive – creating an unfair and uneven playing field.

Challenge #4. The way the eCommerce Directive regulates hosting providers is being used by some platforms – including (but not only) online marketplaces – to either shield themselves from any accountability or not to take any meaningful action for fear of liability.

Challenge #5. Current legislation has gaps to regulate online marketplaces. Little attention is given to online marketplaces’ enrichment from illegal content.

Challenge #6. The new rules may act as a barrier for Member States to correctly address public interest objectives.

For example, in case C-390/18¹⁴, the CJEU ruled Airbnb to be considered as an information society service (Art. 2.a) of the eCommerce Directive). Since France failed to notify the

¹¹ <https://www.beuc.eu/publications/two-thirds-250-products-bought-online-marketplaces-fail-safety-tests-consumer-groups/html>

¹² Defined by the EU Omnibus Directive as “*a service using software, including a website, part of a website or an application, operated by or on behalf of a trader which allows consumers to conclude distance contracts with other traders or consumers*”. Having said that, often the role of the platform is not limited to enabling the conclusion of a contract between sellers and buyers, but it also includes other services such as payment services, fulfilment services, returns processing and complaints handling.

¹³ eCommerce Directive, recital 58.

¹⁴ <http://curia.europa.eu/juris/documents.jsf?num=C-390/18>

Commission about a law requiring an estate agent's professional license to companies like Airbnb, it cannot impose this obligation on Airbnb, as this would breach Article 3.4 b) of the eCommerce Directive. This case showed that the e-Commerce Directive, in putting the internal market first, creates problems for Member States to adopt laws and policies to protect consumers. It is important however to note that the ruling does not mean that Governments cannot impose such measures on companies like Airbnb. The CJEU was clear that the notification obligation in the eCommerce Directive "*is not intended to prevent a Member State from adopting measures falling within its own field of competence and which could affect the freedom to provide services, but to prevent a Member State from impinging on the competence, as a matter of principle, of the Member State where the provider of the information society service concerned is established.*"

Challenge #7. Lack of proper oversight and enforcement.

Digital markets evolve at a fast speed and competent authorities do not seem to cope, have all expertise or resources needed to monitor and tackle the problems of the market.

2.4. Key consumer rights and obligations in a nutshell

The **e-Commerce Directive** has been one of the cornerstones of the internet for a long time. The e-Commerce Directive established the country of origin principle with some important exceptions (notably consumer contracts), key information obligations towards the recipients of services (e.g. consumers), liability exemptions and limitations for online intermediary service providers, amongst other provisions:

- **Article 1 – 3: General provisions**
- **Article 4 – 15: Principles**
 - Section 1: Establishment and information requirements
 - Section 2: Commercial communications
 - Section 3: Online contracts
 - Section 4: Intermediary liability
- **Articles 16 – 20: Implementation**
- **Articles 21 – 24: Final provisions**

Where to find the most important provisions in the e-Commerce Directive?

- **Main objective:** internal market and freedom to provide information society services (Article 1).
- **Other objectives** include "*legal certainty and consumer confidence*" (Recital 7), ensuring a high level of consumer protection and protection of minors (Recital 10)
- **Scope:** without prejudice to consumer protection (Article 1)
- **Definitions** (Article 2)

- **Basic information** to consumers & other recipients (Articles 5, 6, 10)
- **Rights when placing orders online** (Article 11)
- **Intermediary liability principles** (Articles 12-15). The most important principles here are:
 - Hosting providers are not liable for third-party content as long as upon knowledge, they expeditiously remove or disable access to illegal content (Article 14)
 - Prohibition for Member States to impose a general monitoring obligation on providers (Article 15)
- **Codes of conduct** (Article 16)
- **Alternative dispute settlement** (Article 17)
- **Court actions** "to terminate any alleged infringement and to prevent any further impairment of the interests involved" (Article 18)
- **Member State cooperation** (Article 19)
- **Sanctions** (Article 20)

Since the adoption of the eCommerce Directive in 2000, digital services have evolved, raising new challenges. For example, the safe harbour principle is giving some platforms a free space not to be held liable. Some digital service providers are not taking meaningful responsibility or giving consumers proper redress if something goes wrong. Similarly, some voluntary initiatives have delayed much-needed regulatory action. Some of these issues are being addressed under the upcoming Digital Services Act.

Consumer PRO has also developed two other documents on the topics of General Consumer Law and Collective Redress that can complement this chapter in a useful way.

2.5. Outlook: The upcoming Digital Services Act

The upcoming Digital Services Act (DSA) will regulate the obligations of digital services that act as intermediaries in their role of connecting consumers with goods, services, and content.

It aims to better protect consumers and fundamental rights online, establish an efficient transparency and accountability framework for online platforms and thereby foster fairer and more open digital markets.

As opposed to the e-Commerce Directive, the DSA is a Regulation so it will harmonise the rules across the EU and be directly applicable. The new rules should ensure the same level of protection to all citizens in the EU.



Among other things, the DSA will include¹⁵:

- Measures to counter illegal content online, including goods and services, such as a mechanism for users to flag such content, and for platforms to cooperate with “trusted flaggers”;
- New rules on traceability of business users in online marketplaces (also known as “know your business customer obligation”), aimed at better identifying sellers of illegal goods;
- Safeguards for users, including the possibility to challenge platforms' content moderation decisions;
- Additional transparency measures for online platforms, including on the algorithms used for recommendations and on targeted advertising;
- Obligations for very large online platforms to prevent abuse of their systems, in particular by addressing systemic risks and including oversight through independent audits of the measures they take;
- A new oversight structure to address the complexity of the online space in which Member States would have the primary role, supported by a new European Board for Digital Services. For very large online platforms, there would be an enhanced supervision and enforcement role for the Commission.

While the DSA will bring much needed improvements in terms of consumer protection in digital services, one point where there is unlikely to be major changes is on the liability regime for online marketplaces. The DSA will very likely maintain the intermediary liability exemption principles of the eCommerce Directive, albeit with some clarifications and small improvements. Laws and Regulations at EU level

REGULATION / DIRECTIVE	DATE OF APPLICATION	REVIEW / EVALUATION: TYPE OF MEASURE	DUE DATE	COMMENT
eCommerce Directive	17/01/2002 (transposition)	EC re-examination report (Art. 21)	Before 17/07/2003, and thereafter every two years	No formal evaluation is known to us since 2012 . The Commission's 2017 sector enquiry may be interesting from a competition perspective.

¹⁵ This is a generic overview of some of the elements which are expected to be included in the final text of the Regulation, which is still under discussion



		Digital Services Act (DSA)	Proposal published in December 2020 – Currently in final stage of co-decision procedure. Expected to be adopted in 2022	DSA proposal presented in December 2020 together with the Digital Markets Act (DMA) which has specific rules aimed at gatekeeper platforms. Key topics in the DSA from a consumer perspective: liability and responsibility of intermediaries, in particular online marketplaces; know your business customer obligations, procedures for notice and action, transparency requirements, enforcement and coordination between Member States, obligations in relation to targeted advertising and the use of recommender systems.
Platform to Business Regulation (P2B Regulation)	12/07/2020	EC guidelines on ranking transparency requirements (Art. 5)	Published 7 December 2020 Published 7 December 2020	
		EC to encourage codes of conduct (Art. 17)	No date	An analysis of their functioning will be part of the review.
		EC review report (Art. 18)	13/01/2022 and every three years	
Omnibus Directive	28 November 2021 (transposition) 28 May 2022 (application)	Article 7 – Transposition	Article 6 – Reporting by the Commission and review. Report to be published by EC by 28 May 2024, DQ of food and doorstep selling measures.	

2.6. Case law

- **Re: Omnibus Directive:** no case law yet as it will only become applicable as of 28 May 2022. Check the General Consumer Law theoretical background document to find out about case law of other consumer law instruments.
- **Re: eCommerce Directive:** see list of [cases here](#).

2.7. What can consumers do if they have a problem?

- Go back to the seller/platform directly (this step is not obligatory).
- Alternative Dispute Resolution (ADR) possible (this step is not obligatory).



- Member State competent authorities: it varies from country to country and from topic to topic.

2.8. Further resources – factsheets, publications, links

- European Commission presentation about the instruments and objectives followed in the E-Commerce Directive (see [here](#))
- BEUC position paper Ensuring consumer protection in the platform economy: ([here](#))
- BEUC position paper Collaborative economy ([here](#))
- BEUC position paper on making the Digital Services Act work for consumers ([here](#))
- BEUC position paper on the Digital Services Act proposal ([here](#))
- BEUC factsheet: The proposed Digital Services Act – Better protecting consumers ([here](#))
- European Parliament Briefing on the Digital Services Act proposal ([here](#))
- European Commission – Q&A document on the Digital Services Act ([here](#))



3. INTERNET OF THINGS (IOT)

3.1. Introduction & History

In the span of the last few years, connected devices have become ubiquitous in the lives of many consumers. Whereas before we would normally be in front of a computer to access the internet, we now carry internet-connected smartphones everywhere we go. Simultaneously, an increasing amount of the everyday devices around us are being fitted with sensors and connected to the internet. From connected coffee makers and security cameras to cars and medical devices, the rise of connected devices is commonly known as the “internet of things”, or IoT.

3.2. Why IOT matter to consumers

In recent years, connected devices have become omnipresent in the lives of many consumers, and the rise of connected devices is changing the way we conduct our lives. While digitalisation of devices provides many benefits for consumers, the risks and challenges it brings are equally important, if not even greater. For example, what happens when the service provider of your smart home system decides to shut down their servers? And who is responsible if your smart TV is compromised or rendered useless because of a lack of software updates? And what about the impact on our privacy?



It is therefore important to develop clear and forward-looking EU policies and a legal framework that ensure that consumer rights are maintained in this connected environment.

3.3. Main challenges within IOT

Connecting large amounts of devices to the internet raises both opportunities and risks for consumers. The interconnected world promises increased comfort, seamless experiences, and potentially significant improvements to quality of life. Aggregated information from these devices could also lead to new insights in areas such as medical science, artificial intelligence, and city planning.

For example, a smart home filled with connected devices and sensors may learn the habits and preferences of its owner, and tailor its functionality accordingly. Simultaneously, the different individual devices can communicate with each other, so that for example a low cardiac rhythm detected by a smart watch generates an urgent message to the closest hospital. Furthermore, the capability of remote monitoring of devices through the internet can help individuals who are in need of assistance retain their independence, for example by unlocking doors remotely without the need of walking to the door. In sectors such as industry and health, the internet of things is set to have potentially transformative effects on efficiency and information accumulation.

But the challenges that connected devices bring are manifold from a consumer perspective. They touch upon a wide range of policy areas and issues: privacy and data protection, cybersecurity, product obsolescence, sustainability and energy consumption, competition, safety, consumer rights, etc.

For example, connected devices will typically collect vast amounts of data about its users and its environment. This widespread data collection raises a number of pressing concerns related to data protection and privacy. As more aspects of our lives are increasingly embedded in a wider network of sensors and devices, the potential risks and scope of data breaches and cyberattacks also grow. Every new device we connect to the internet adds another potential attack surface, and the chain of devices is often only as strong as its weakest link. The emergence and implementation of artificial intelligence in IoT technologies also poses challenges related to fairness, accountability, and more.

Other challenges that are introduced or exacerbated through the internet of things include artificial limitation of product lifecycles, lock-in effects and product liability.

Also, networked devices have an increased energy consumption due to their required networking components. A large part of this energy consumption arises from the continuous responsiveness of the devices via the network (idle mode). Friedli et al. (2016) projected that global standby losses will increase from 7.5 TWh in 2015 to 47 TWh in 2025, based on the standby consumption of networked devices that are permanently connected to the power grid.¹⁶

3.4. Key consumer rights and obligations in a nutshell

When it comes to connected devices, consumer rights applicable to non-connected devices also apply. For example, rules on legal guarantee (Digital Content Directive, Sales of Goods Directive) apply to IoT consumer products. Rules on consumer information (Consumer Rights Directive) at the point of sale also apply. Refer to the complementary theoretical background document on General Consumer Law for more about the Sales of Goods Directive and Consumer Rights Directive. To a certain extent¹⁷, rules of product safety legislation also apply to IoT devices.

However, due to the connectivity of these devices, specific obligations apply:

- 1) Firstly, devices that collect personal data about consumers have to be sure that they process this data according to the rules set forth in the GDPR. These rules include, but are not limited to, the principles of data minimisation, purpose limitation and data protection by design, and the obligation to obtain user consent depending on the purposes of data processing.¹⁸

¹⁶https://nachhaltigwirtschaften.at/resources/iea_pdf/reports/iea_4e_edna_energy_efficiency_of_the_internet_of_things_technical_report.pdf

¹⁷ These rules state that all devices need to be safe. There is not an agreement on whether the concept of 'safety' shall also include 'security'. The agreed position is that product safety legislation applies to connected devices if the security vulnerability in the device leads to a safety concern (e.g. hacker exploits the vulnerability in the fire alarm to turn it off. If a fire erupts, the occupants of a household would be in physical danger).

¹⁸ For more information on data protection and General Data Protection Regulation (GDPR), see Chapter 1.



- 2) Secondly, according to the Radio Equipment Directive, as of 2024, manufacturers of connected devices will have to ensure that their devices display a certain level of security. These measures shall ensure that the devices (i) do not harm the network causing an unacceptable degradation of service; (ii) incorporate safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected and (iii) support certain features ensuring protection from fraud such as ransomware.
- 3) As per the Digital Content Directive, connected devices must be supplied with updates, including security updates, for the period of time that consumers can reasonably expect. The length of this obligation is linked to the legal guarantee period but can also go beyond it.
- 4) Fourthly, under the Cybersecurity Act, when certification schemes exist and apply to the connected device in question, the manufacturer of that device shall inform the consumer about the period during which security support will be offered to end users, in particular as regards the availability of cybersecurity related updates.
- 5) Consumers should have a clear expectation that access to Internet services are provided in a neutral, non-discriminatory way according to the Open Internet Regulation. Internet service providers must treat all internet traffic equally without discrimination, restriction or interference ('net neutrality'). Keeping internet access open and neutral is essential if we are to exercise our fundamental freedoms and democratic rights to participate in today's interconnected online societies. It is also a precondition to benefit from the Internet of Things. Consumers need an unrestricted and neutral internet to use their connected devices to access news and cultural content or to shop without restrictions.
- 6) When it comes to rules on Product Liability, the relevant directive – Product Liability Directive - was drafted back in 1985, long before one could consider the use of connected devices, let alone foresee the challenges ahead. It is no longer adapted to tackle the challenges by the internet of things and to ensure compensation to consumers when things go wrong. The process to review this directive is ongoing. In April 2020, BEUC made several recommendations to ensure that EU product liability rules remain fit for consumers in the digital age and to IoT.¹⁹

3.5. Laws and regulations at EU level

- [Directive 2014/53/EU](#) of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC
- [Regulation \(EU\) 2019/881](#) of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and

¹⁹ BEUC, *Product liability 2.0 - How to make EU rules fit for consumers in the digital age*, April 2020, www.beuc.eu/publications/product-liability-20-how-make-eu-rules-fit-consumers-digital-age/html

communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

- [Directive 2001/95/EC](#) of the European Parliament and of the Council of 3 December 2001 on general product safety
- [Directive \(EU\) 2019/770](#) of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services
- Open Internet Regulation ([Regulation \(EU\) 2015/2120](#)) of 25 November 2015.
- [Regulation \(EU\) 2015/2120](#) laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services
- European Commission's report on [consumer Internet of Things sector inquiry](#)

* Other relevant laws covered in other modules, such as GDPR and the consumer rights acquis are not referenced here but as explained above, are also applicable in an IoT context as any other product or service. E.g. if a connected device processes personal data, it will have to comply with the GDPR.

3.6. Case law

When it comes to 'net neutrality' (see Point 5 of Chapter 3.4), the Court of Justice of the EU, recently ruled in Cases C-854/19, C-5/20 and C-34/20 that offers applying a 'zero-tariff'²⁰ to specific apps - and therefore limitations that derive from the activation of these options (on bandwidth, tethering or on use when roaming) – are in violation of Article 3(3) of the Open Internet Regulation and, therefore, are illegal under EU law. Service providers should therefore review their commercial practices in line with this interpretation to ensure that they fully respect EU rules on net neutrality. A similar reasoning could be applied by the Court to service providers that offer a 'zero-tariff' for the apps associated with connected devices (e.g. in the context of a marketing campaign, an internet service provider offers an advantageous tariff, i.e., zero tariff, to the app used to control a smart camera).

3.7. What can consumers do if they have a problem?

Several laws apply to connected devices. Depending on the applicable law, consumers will have different options.

- If it is a problem related to their personal data (see Point 1) in Chapter 3.4), the GDPR applies.²¹
- According to the Radio Equipment Directive, if there is a problem with the security of their devices (see Point 2 in Chapter 3.4), as of 2024, consumers will be able to notify their national market surveillance authorities (often the telecommunications authority), who

²⁰ 'Zero-tariff' is a commercial practice according to which an internet service provider applies a 'zero tariff' (or a tariff that is more advantageous) to all or part of the data traffic associated with an application or category of specific applications, offered by partners of that internet service provider.

²¹ See previous footnote.

shall then start an investigation into that specific device. The decision of the market surveillance authority can go as far as to order the withdrawal of that product from the market.

- If the device was not supplied in accordance with the expectations of the consumers when it comes to the provision of security updates (see Point 3 in Chapter 3.4), consumers shall have the right to terminate the contract, receive a proportionate reduction in price or require that the device is brought into conformity (see Digital Content Directive).
- Under the Cybersecurity Act, if the provision of security updates is shorter than announced by the manufacturer (see Point 4 in Chapter 3.4), consumers shall be able to lodge a complaint with a national body. If consumers are unhappy with the decision taken by the national body, they shall have the right to an effective judicial remedy.
- If net neutrality is not respected (see Point 5 in Chapter 3.4), consumers can complain to their telecommunications' regulatory authority, who will have to act upon them.

3.8. Further resources – factsheets, publications, links

European Commission Staff Working Document - [Advancing the Internet of Things in Europe](#)

European Commission [Sector Inquiry into the consumer Internet of Things](#) (IoT)

BEUC position paper: [Protecting European consumers in the world of connected devices](#)

BEUC factsheet: [Ensuring cybersecure consumer products](#)

AK EUROPA - [Consumers' expectations of the Internet of Things](#)



This document has been produced under a service contract with the European Commission. The content of it represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

