AK EUROPA

**Position Paper**
**August 2020**
**Digital**

# Side-letter to the European Commission on the Public Consultation concerning the Digital Services Act

# The AK's position

In its work programme, the European Commission has announced the publication of a legal proposal on digital services this year. In the view of the Austrian Federal Chamber of Labour (AK), such a legal proposal is urgently needed and has been overdue for years.

Some of the legal standards currently applied to online platforms and other digital services were adopted around 20 years ago and fall far short of the minimum requirements for the digital world in terms of employment, social, consumer protection, tax and competition policy.

The AK welcomes the opportunity to participate in the public consultation on the planned law on digital services. In the AK's view, however, essential questions are lacking, which must in any case be included in the deliberations on the law on digital services. In other cases, legal loopholes are addressed, but do not sufficiently cover the existing problems in the digital space.

## I. End precarious employment on digital platforms

Module 5 of the consultation deals with workers in digital platforms. This is welcome, as many platforms refuse to recognise their employer status. **Basic labour rights** are thus **put into question.** Work for platforms must not lead to a systematic undercutting of national statutory minimum and collective agreement wages, which is often the case at present. Working conditions must be designed in a humane manner, and mental and physical performance must not be overtaxed. The recognition of these basic principles must also be enshrined in the Digital Services Act. Not least because a significant increase in the number of people working for a digital platform can be expected in the coming years.

From the AK point of view, however, the expectation of the European Commission in the first part of Module 5 that many employees of online platforms will participate in the consultation and answer the questions is not comprehensible. Moreover, it is **incomprehensible why** the **questions are only addressed to "self-employed individuals" and not to employees and bogus self-employed persons.** Employees in these areas are not EU experts who regularly inform themselves about EU legislation and participate in surveys. Some of those addressed will also have language problems when answering the consultation form, for example if the person is originally from a third country. In extreme cases, online platforms may ask their employees to participate in the consultation and try to influence the responses of the people working for them. The **involvement of trade unions and works councils** would therefore have been urgently needed for this part of the consultation.

It is doubtful whether the results of this part of Module 5 are meaningful enough due to a possibly low number of participants or a possible influence of the employer.

From AK's point of view, the **following minimum criteria** in the legal framework for the digital services sector must be fulfilled in any case to ensure adequate protection of employees in the online platform industry:

- The statement that in case of doubt there is an employment relationship with the platform as a dependent employee.
- Collective agreement provisions or minimum wage regulations apply.
- The same worker protection rules apply to digital service providers as to traditional sectors of the economy. In addition, digital platforms must provide for compulsory accident insurance for their employees.
- The platform is responsible for the payment of wage tax, social security contributions and all other wage-related charges for its employees.
- Information obligations of platforms towards

authorities and social security institutions - even if there is no employment relationship with them but with the benefit recipients

- In order to avoid wage dumping, it must be ensured that the remuneration or fees paid to self-employed persons are not lower than those paid to employees performing the same or similar activities.
- Application of the right to equal treatment and the obligation of equal pay.
- Standby times and search times must also count as working time
- The use of competition and exclusivity clauses and all other unfair clauses in employment contracts or contracts with self-employed persons must be excluded from the outset.
- Disclosure of how ratings about platform workers come about, including the possibility to correct falsified ratings.
- In the event of a dispute, self-employed persons must be able to contact the regulatory authority (see below) and receive appropriate support.

## II. Ensure fair competition

### Close loopholes, create mandatory digital sites

It must be ensured that in the case of digital services, the regulations in the country in which the digital company is economically active apply. This is the only way to avoid a ruinous European location race. However, this question is missing in the consultation. A lack of regulations creates unjustified privileges for the digital industry - for example in the area of employee protection, labour law, consumer protection or tax law. The obligation to **set up a digital branch** in the countries where digital companies are active makes it much easier to avoid circumvention of protection regulations for employees and consumers and of tax and duty obligations by some digital companies.

### Take account of tax and duty obligations

Especially in the case of international digital corporations, it can be observed time and again that they **do not pay their taxes in the country in which they are economically active.** Instead, they switch to other countries with lower or no taxation. In addition, some platforms refuse to exchange data with authorities, which is necessary to collect due fees and taxes.
Considerations on the tax and duty obligations of digital service providers are missing from the consultation. However, the new law on digital services must ensure that online platforms also pay their fair share of taxes and that traditional companies are no longer disadvantaged by the current status quo.

### Competition law - ex-ante regulatory instrument for large online platforms

Module 3 of the EU consultation procedure deals with the power of digital gatekeeper platforms and the possible ex-ante regulation of large online platforms with significant network effects. The AK would like to make the following supplementary comments on this section:

The modern global economy poses new challenges for competition law in Europe and worldwide. Some of the legal standards currently applied to online platforms and other digital services were adopted 20 years ago. The AK therefore welcomes the EU Commission's initiatives to identify the need for reform in the course of several complementary consultations and to draw up concrete proposals on this basis.

The new competition instruments under discussion (ex-ante regulation of platforms, new competition tools as well as reform considerations regarding market definition) can help to ensure that existing competition problems, especially in the digital economy, are tackled quickly and effectively and that future developments are examined in greater detail. However, fair competitive conditions are not only needed within the digital economy, but also between the modern and the traditional economy (e.g. between stationary and online trade). Additional measures are therefore needed to prevent distortions of competition through tax evasion and wage and social dumping.

### Revision of the platform-to-business Regulation (2019/1150)

Regulation (EU) 2019/1150 to promote fairness and transparency for commercial users of online intermediary services entered into force in July 2020 and provides good regulatory approaches to protect third party providers on platforms. In the opinion of the AK, this regulation should also be extended to consumers. For example, with regard to the disclosure of blocking reasons (Art 3/1c and Art 4) it would also make sense to apply it to private individuals (e.g. online auctions, social media and private app developers vis-à-vis app stores). The transparency

laid down in Art 7 of the Regulation with regard to the differentiated treatment of own goods and those of competitors should also be applied to consumers. The type and scope of data access by the intermediary service and third party providers (Art 9) should also be explained to consumers.
From AK's point of view, however, the revision of Regulation 2019/1150 should only be seen as an additional step in the regulatory discussion. The problems arising from the power of digital gatekeeper platforms are far more diverse and can only be solved by establishing specific regulatory authorities at both national and European level.

### Horizontal framework enabling regulators to obtain information from major online platforms acting as "gatekeepers

In the opinion of the AK, it is of enormous importance that future regulatory authorities are enabled to obtain information from online platforms that is necessary in view of their regulatory tasks. However, this approach should also only be understood in connection with the following point:

**New and flexible ex-ante regulatory frameworks for large online platforms acting as "gatekeepers**

- Prohibition or restriction of certain u**nfair trading practices** ("black list")
- **Tailor-made remedies** for large online platforms acting as "gatekeepers" when necessary and justified.

In the AK's view, sector-specific ex-ante regulations for market-dominant Internet platforms are urgently needed to complement existing competition law. This should ensure that the "rules of the game" are proactively set in two- or multilateral markets in order to meet the requirements of rapidly advancing digitisation.

Internet platforms with high market power have the characteristics of classic infrastructures. While electricity, telecommunications or railway networks are regulated, large online platforms set the rules themselves and act as private rule-setters and gatekeepers. In addition, all Internet platforms with market power have in common that they possess a large pool of data relevant to competition and thus have the data infrastructure in addition to the digital infrastructure. The competition authorities have already concluded or initiated a number of important proceedings. However, these proceedings take too long to establish fair competition in a timely manner. The cases of abuse taken up have in common that the respectively dominant platform operator (such as Amazon, Google or Facebook) abused its dominant position. The abuse control of competition law therefore regularly has an ex-post effect and ultimately represents only reactive action.

The creation of regulatory authorities at European and national level is necessary in order to achieve the meta-goals mentioned by the EU Commission. These are, in particular, an open, democratic and sustainable society as well as a technology that serves the people. Especially in the area of media-specific content, increased vigilance is needed. This is because online platforms often do not offer the editorial independence with the corresponding duty of care and control (e.g. fake news). Algorithm-based, non-transparent information selection can also severely restrict the diversity of opinions. Platform operators have to take responsibility for fraudulent actions, the distribution of fake news as well as hate and agitation. Platform operators need clear guidelines with regard to editorial due diligence to ensure the quality of the media and diversity of opinion on the one hand, and legal framework conditions on how to deal with the distribution of fake news and hate on the other.

Ex-ante regulations are also necessary in the context of the development of Digital Innovation Centres and Artificial Intelligence (AI). The involvement of data protection authorities should be provided for, especially in the case of complex issues relating to data. Another important area of activity would be the establishment of dispute resolution mechanisms.

## 3. Consumer protection must be strengthened

The safeguarding and further development of the sector-specific level of consumer protection in Europe is a particular concern of the AK. The AK is especially committed to ensure that the needs of consumers for **up-to-date protection against non-transparency, misleading, unconscionability and fraud on the internet** are adequately taken into account.

### Transparency of rankings on all platforms

**This already exists:** There are transparency regulations for rankings (their parameters and weighting) for so-called online marketplaces which are used to process online purchases (Revision of the Directive 2005/29 EC on unfair commercial practices) and search engines (Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services).

**What is missing:** There is no remedy for non-transparent, algorithmic ranking of content in the case of platforms that provide **(media) content that is user-generated or provided by third parties in the broadest sense.** No matter whether YouTube, Facebook, Alexa or Netflix and many more – for users, it is not clear which rules define how content is transmitted. Especially for news-relevant content (such as news feeds), which is a main source of information for many consumers; one can expect clarity on the factors used in rankings. To use transparency as a means against manipulation of opinions is also extremely important in terms of democratic policy. It also requires fairness towards conventional media providers who disclose their editorial policies.

## Finally ensure a uniform level of regulation for online advertising

**This already exists:** The e-Commerce Directive contains some principles concerning advertising borrowed from classical media law. The respect of these principles continues to be of fundamental importance for consumers. However, they are far from sufficient to provide up-to-date protection against manipulation, harassment and deception. The Directive requires information society services to identify commercial communications in accordance with the principle of separation between advertising and editorial content. The client behind the advertising must also be clearly identifiable. Finally, Member States must offer Robinson lists to consumers who do not wish to receive advertising. This measure is correct and important in its approach, but in practice it has remained practically a dead letter. More detailed advertising regulations exist for audio-visual media providers only (AVMSD Directive (EU) 2018/1808). With the latest revision of the Directive, platforms such as YouTube will be included in the scope. Platforms that do not contain predominantly audio-visual content are not covered.

**What is missing:** The above-mentioned advertising principles (labelling, separation, disclosure of the client, compliance with a centrally managed general opt-out on advertising) are systematically violated, given that there is an almost complete lack of effective control and tangible sanctions. Consumers are not just exposed to a lack of transparency, manipulation, harassment and illegal advertising content. Traditional media that adhere to advertising rules are grossly disadvantaged by unfair online advertising forms or content. **Strict supervision and sanctions against infringements** must therefore be an important cornerstone when revising the Directive.

In order to truly do justice to the right of self-determination of Internet users, the **Robinson list for e-mail advertising** would have to become **a real "stop tracking" tool for every form of online advertising.** A centrally administered opt-out possibility can currently only be set up for unsolicited mail advertising – however, other directives prohibit spam anyway and unsolicited mail advertising is subject to an opt-in condition (consumer consent) in many Member States. Anyone who does not appreciate online advertising generally, and sees it as a nuisance, currently has no reasonable means of expressing this attitude simply and effectively. Intermediaries from the online advertising industry earn money from forced advertising. However, in the case of Internet users who are not advertising affine, it completely misses the objectives of the clients.

Currently, consumers have to struggle with every service and in an unacceptable manner with endless declarations, difficult settings and enormous deficits in data protection and media law.

Those who do not want their digital traces to be tracked across the Internet for advertising purposes in order to create individual behavioural profiles and transmit the corresponding advertising should be able to register in a central list. All online services that target their offers to the country of residence of the persons registered on the list must respect their wishes.

Moreover, it is high time for **a uniform, strict level of regulation for online advertising,** regardless of the sites where the advertising is played. So far there are only a few detailed rules for advertising in audio-visual media. Consumers do not care which website or app they visit. Their need is always the same: to be protected from advertising that is non-transparent, aggressive or harmful to health, the environment, youth, etc.

Since **advertising for dubious or fraudulent services** is starting to dominate, it is essential to clarify **responsibilities in the chain of advertising service providers and platforms.** Since platforms are involved in the marketing practices of online advertising through the behavioural profiles of their users and a share in advertising revenues, they should be required to assume greater responsibility with regard to illegal advertising. They should provide **tools to clearly identify** advertisements and their clients, which advertisers must be obliged to use. They should also be required to carry out prior **automated checks on advertising for obvious illegal activities** (e.g. fake shops, prohibited goods – especially pirated goods, data theft and distribution of malware, etc.). In

contrast to other content, there is hardly any risk that automated filters will violate information and personal rights protected as fundamental rights.

Other **websites with third-party advertising** must at least establish a **complaints mechanism** to ensure that information about advertising violations reaches the advertising intermediaries behind it quickly.

The **online advertising industry that places advertising on websites is liable** for the rapid establishment of a lawful state (modification or ban of incriminated advertising).

## Consumers should also benefit from the protection of the Platform to Buisness Regulation

**This already exists:** The EU regulation only protects third-party providers in online marketplaces from a lack of transparency and discrimination.

**What is missing:** Numerous protective standards are also useful for consumers: e.g. **disclosure of reasons for blocking** on platforms for private ratings, with user-generated content or commentary function (Art 3/1c and Art 4). The explanation of the effects of **differentiated treatment** of own goods and those of competitors (Art 7) must also be disclosed to consumers. The **type and scope of data access** by the intermediary service and third-party providers (Art 9) should also be explained to consumers by the platform in a comprehensible manner. Currently there are considerable deficits, e.g. in the app stores or third-party applications, for language assistants such as Alexa or Siri, which only refer to the privacy statements of the respective developers. Platforms contractually oblige developers to comply with laws anyway, including those relating to data protection and data security. They should inform consumers of which customer data the platform and developers share and which contractual obligations they control and how. In case of violations, the platform shall be jointly liable with the developer.

## Ensure net neutrality at platform level

**This already exists:** Internet operators are obliged to respect network neutrality (Telecoms Single Market Reg. (EU) 2015/2120). Net neutrality means that, in principle, all data is treated equally when transmitted within networks. Videos and e-mails are transported through the network to the user at the same speed as websites, Internet phone calls and online banking. Net neutrality also means that offers from a particular company are not given preferential treatment, i.e. that only one particular video service is transmitted at an accelerated rate.

**What is missing: Platforms with gatekeeper function** also need the obligation to comply with the principle of **net neutrality.** A supervisory authority must monitor platforms' compliance. For example, it is necessary to control the rules by which content delivery platforms play out content or language assistants react to commands. The aim should be to ensure transparency, freedom of choice and diversity for consumers.

## Fight against cybercrime on platforms

There is an urgent need for remedial action to combat cybercrime on platforms. Indeed, the total number and variety of forms of fraud on the Internet (data and identity theft, fake shops, pre-payment fraud, etc.) is increasing steadily and sharply according to the crime reports of the Member States. This leads to a considerable loss of consumer confidence in the safe use of online services in general. Internet fraud usually has a cross-border dimension, but it also harms consumers, even serious smaller online providers, from whom consumers are increasingly reluctant to order out of caution. The beneficiaries of this growing insecurity are a few large, well-known intermediary platforms such as Amazon.

**This already exists:** In Austria, for example, there is the initiative **"Watchlist Internet"** (www.watchlist-internet.at), **which sees itself as an independent information platform providing information on Internet fraud and fraud-like online traps.** It lists current Internet fraud cases and gives recommendations on how to protect yourself from common scams. Victims of Internet fraud receive concrete instructions for further steps. Current main topics include: subscription traps, classified ad fraud, phishing, rip-offs via mobile and smartphone, fake shops, brand forgery, scamming or advance payment fraud, Facebook fraud, fake bills, fake warnings, ransom Trojans. The Watchlist helps Internet users to **know more about online fraud and to learn how to deal more competently with fraud tricks.** This increases confidence in their own online competence as well as their trust in the Internet. Via a reporting form, Internet users can report traps themselves. Through push messages, interested parties are informed daily about the latest scam sites.

**What is missing:** There is a need of **an EU-wide initiative comparable to the Watchlist Internet,** which is perceived as a task in the public interest and is sufficiently funded by the EU or the Member States. In addition, closer cooperation between such a European "Watchlist" and the individual law enforcement authorities should be targeted. On the basis of the complaints received by the Watchlist and its searches

as “trusted flags”, judicial orders to block incriminated sites can be carried out more quickly.

**Measures against the enormous emergence of fake shops** are urgent. Fake shops are difficult to recognise at first glance. Some of them are copies of real existing websites, they appear serious at first glance and therefore rarely leave the buyer in doubt about their authenticity. With well-copied product images, fake quality marks and a professional appearance, fake shops gain the trust of online shoppers and entice them to buy. Another lure is the apparently particularly low price of the product they are looking for. After prepayment has been made, inferior goods are shipped at an inflated price or - far more often - the product is not delivered at all. Even small tests show the extent of the problem: If you search for a certain product category on Google Image Search, you will often find considerably more fraudulent fake shops than serious offers. In Google text searches, fraudulent offers are often at the top of the list even before the first serious offer. In Austria, there is a cooperation between science and consumer protection (Verein Internetombudsmann) with the aim of using algorithms to identify fake shops and fakes of e-commerce quality marks more quickly on the basis of typical recurring features. The hit rate is already very promising in the current test phase.

Against this background, intermediary platforms should be obliged to automatically filter out easily recognisable fraudulent third-party providers on their platform even before consumers see these offers.

**Platforms should especially**

- clarify the identity of commercial third parties by means of register comparisons, documents etc.
- immediately investigate a case of fraud reported by consumers.
- take out insurance to compensate consumers if dubious third party providers are activated on the platform and evade their responsibility in the event of damage.
- prevent reported illegal offers from appearing again.

Systematic action must also be taken against individual fraudulent websites apart of intermediary platforms: Consumers and consumer organisations should be able to report suspected cases of abuse to **public or private reporting offices with “trusted flagger” status** at a low threshold. Through close cooperation with law enforcement agencies and courts, site closures should be implemented quickly after the reports have been examined. In cooperation with app developers, there should be **an EU-wide app** which, in line with the Austrian pilot project, assesses the reliabilities of websites according to characteristics which are continuously updated. A green-yellow-red traffic light makes it visible whether the website is trustworthy, should be critically questioned or not be used as a probable fake shop.

According to the motto **“know your customer”, providers of online marketplaces should check commercial third-party providers before unlocking them:** Intermediary platforms have an enormous amount of information on end-consumers (behavioural profiles on tracking methods, creditworthiness queries with credit agencies, purchase history etc). Most platform operators do not screen the third-party providers activated on the platforms at all or at least not very precisely. For example, with regard to online trading platforms such as Amazon, consumer complaints about fraudulent third-party providers (mostly from third countries such as China) are increasing. In addition, also the two central app shops reliably ensure that allegedly free online games for children/young people contain reliable information on in-app purchases prior to download.

While national trading platforms require a wide range of documents from third-party providers before they are activated after a lengthy review process, some international trading platforms often take less than two minutes to register a new shop. The extremely inconsistent due diligence standards are equally disadvantageous for consumers and for smaller European platforms, which have to carry out a much greater amount of checking in the course of registration. In accordance with the principle of “know your customer”, intermediary platforms for goods, services or digital content should be obliged to check third-party providers for obvious misrepresentations and illegalities (branch address, trade register entry, company register, fraudulent fake offer etc.) before activating their offer. Without authorised representatives within the EU, legal enforcement steps against providers from third countries are futile and pointless. Against this background, providers from third countries wishing to enter the EU market must be obliged to appoint a representative with a legally enforceable address within the EU. Intermediary platforms for goods, services and digital content should be obliged to check this information. If the “know your customer” requirements are disregarded by an intermediary platform, the platform itself must be liable for disadvantages and damages incurred by consumers as a result of this negligent prior checking.

## Transparency through a uniform european corporate register

**This already exists:** The business registers of the EU Member States have in principle been interconnected since June 2017 in accordance with Directive 2012/17/EU and are accessible via the "European Justice", the EU's justice portal as the EU Business Registers Interconnection System (BRIS). This should make it easy to find public limited companies, limited liability companies and their branches or companies registered as European companies (Societas Europaea - SE).

**What is missing:** However, not all EU Member States have so far allowed access to their registers. The quality of company information varies greatly from country to country. The Member States must therefore first ensure that the information is up-to-date and reliable. Moreover, every online provider should be obliged to provide a clearly visible link to his entry in the company register or to the respective entry in a trade register. Platforms that do not have a branch in the EU must appoint an authorised representative with a legally enforceable address within the EU. By analogy with Art 27 DSGVO, the representative should be a natural or legal person established in the EU who has been instructed in writing by the online provider and represents the online provider with regard to the obligation to comply with EU law (consumer protection standards, trade law etc.). Providers from third countries should enter their permanent representatives with a legally enforceable address in the EU in a centrally accessible EU register.

## Graduated liability according to the type of platform

**This already exists:** The maxim **not to impose general, blanket obligations** to check in advance on Internet access and host providers in cases where fundamental rights are affected has proved its worth in principle and must be **retained** in relation to host providers who carry out activities sensitive to fundamental rights (Art. 15 of the e-Commerce Directive). In other words: In the case of social media and generally platforms based on user-generated content or similar to traditional communication services, the prohibition of general monitoring obligations should definitely be maintained. Freedom of opinion and information or the observance of the secrecy of communication are of paramount importance in this case. When weighing up the pros and cons of preventive filtering measures, the concerns about the associated restrictions on fundamental rights and freedoms under the ECHR far outweigh the concerns about the consequences. The AK considers "proactive measures" (essentially an algorithm control), such as those contained in the EU Regulation on combating terrorist online content, to be questionable from a fundamental rights perspective. The **AK rejects further derogations of Art 15 on the control of content** subject to freedom of opinion and information, data protection and privacy.

**This is missing:** However, there should be exceptions to the principle of Art 15 in areas in which the **protection of fundamental rights does not play a special role: these include online marketplaces and advertising practices.** With regard to commercial advertising distributed on platforms, an obligatory prior check (compliance with labelling requirements under advertising law, obviously illegal content) can and should apply without any fundamental rights concerns. Which liability rules apply should depend on the type of platform. In the case of intermediary platforms - such as online marketplaces - consumers are exposed to a variety of considerable risks of damage - they range from financial to health impairments (from advance payment fraud to online sales of counterfeit drugs that are dangerous to health). If platforms do not comply with their obligation to clearly identify third-party providers on their platforms and not to activate fraudulent offers that are easily identifiable in the course of a preliminary examination, they should themselves be liable for the damages incurred by consumers due to the lack of due diligence of the platform providers.

## Product liability for platforms

**This already exists:** The EU Product Liability Directive is 35 years old. Therefore, it does not provide adequate answers with regard to distribution structures in online trade and contains unsatisfactory protection gaps for consumers who purchase goods via platforms of traders or manufacturers based outside the EU (above all increasingly in China).

**This is missing:** Joint and several liability should also be provided for the "fulfilment" service provider (storage, packaging, addressing and dispatch of products to which they have no ownership rights, with the exception of conventional postal services) alongside the manufacturer (Art. 3 (1) Product Liability Directive) and the importer (Art. 3 (2) Product Liability Directive). However, even in the case of platform operators who do not provide fulfilment services, joint and several liability based on the model of importer liability (Art. 3 (2) of the Product Liability Directive) seems appropriate. As far as platforms allow providers from third countries, the risk of a claim under the Product Liability Directive is reasonable. Otherwise consumers have absolutely no chance of enforcing legal claims against, for example, US

or Chinese providers. With the help of algorithmic risk assessments (e.g. drugs, electrical appliances from certain third countries, etc.), platform providers would certainly be in a position to prevent dangerous products from entering the marketplace in the first place. They can also pass on such financial risks to their commercial platform users (e.g. calculate the amount of the commission according to whether the product in question poses a high risk) and take out risk insurance.

## Joint liability of platforms

**This is missing:** Platform operators should possibly take responsibility for compliance with EU rules themselves - through joint and several liability of the platform for infringements of rights by the third party providers they have activated. Art. 20 of the Draft Model Rules of the European Law Institute (https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Model_Rules_on_Online_Platforms.pdf) contains a proposed regulation on the liability of platform operators, which seeks a fair balance of interests between the parties involved. According to this, the joint and several liability of the platform provider applies if the consumer "can reasonably confide at the platform operator has a dominant influence on the provider". This requirement is substantiated by a list of criteria.

## Detailed rules for „Notice and Takedown"

**This already exists:** The e-commerce Directive already contains a so-called "Notice and Takedown" procedure. Internet operators can benefit from a relief from liability if they remove or block access to information as quickly as possible once they become aware of its illegal nature. The rules apply to any kind of illegal or unlawful content. However, service providers do not act as internet police here – they must not be forced to carry out general, active monitoring of all content. "Notice and Action" mechanisms have a direct impact on freedom of expression. Currently, access and host operators have to decide when and how content is removed from the network. They often have to make a decision between competing rights and interests. Since companies cannot replace courts in this matter, "privatised law enforcement" must be rejected.

**What is missing:** Platforms that refuse to delete content quickly can be held liable for such content. Therefore, they tend to delete too much rather than too little under pressure. The danger of **"overblocking" platforms** becomes apparent with the implementation of the Copyright Directive. It goes without saying that the platforms need to be given instructions to block or delete illegal content immediately after they have become aware of it. However, there is also a need for **mechanisms of compensation** to ensure that there is no excessive deletion of legitimate contributions on the Internet. The German Network Enforcement Act, which is intended to prevent hate and fake content, is also caught between faster law enforcement and the protection of freedom of opinion. In any case, careful clarification in conformity with fundamental rights requires the decision-making work of independent bodies. It is essential to provide criteria for the composition of the bodies that decide on blocking and deletion. Arbitration boards enjoy broad acceptance especially when the circles concerned (i.e. also consumer protectionists) are involved in the decision-making process. This is to ensure that it is not the platforms themselves that decide, but rather independence, expertise, annual reporting obligations and supervision by a state body. Access to review by the courts must be open to the participants in the conciliation procedure. Furthermore, platforms must be obliged to disclose their (algorithm-controlled) decision-making processes regarding the whereabouts or removal of content and to make documentation of their individual decisions available to the appropriate authorities (data protection, media, criminal law authorities, etc.).

## Role clarity on platforms

**This already exists:** for Internet users who conclude contracts for goods, services or digital content on platforms, it is often not clear whether a contract is concluded with the platform operator or a third party. The first draft of the Consumer Rights Directive provided in Art. 7 for an obligation to provide information on the contractual role, which was not included in the adopted version. The Modernisation Directive also does not contain a corresponding transparency rule on the distribution of roles under contract law. According to Art 6a (1) lit d VR, information must be provided "on how the obligations arising from the contract are divided between the third party offering the goods, services or digital content and the provider of the online marketplace. A clearly visible labelling requirements (outside of GTC information) is not necessarily to be derived from this.

**This is missing:** platform providers should be required to clearly mark when a **contract is concluded with a third party.** They must also provide consumers with reliable details about the contractual partner. For example, it is important for consumers to know whether a **third party provider is an entrepreneur or a private person**, as it depends on whether a contractual right of withdrawal is free of charge or not. Although the EU Modernisation Directive

adopted in April 2019 intends that providers of online marketplaces must inform whether their contractual partner is an entrepreneur. However, they do not have to check the self-reported information of the third-party provider. The protection provided by the norm is therefore far too low.

## Unforgeable valuation system

**This already exists:** there are no clear exercise rules, such as concrete obligations to design rankings, comparisons and evaluation systems. The remedy against manipulation and misleading consumers is currently the prohibition of deception under competition law. It is difficult to prove the violation of unfair competition law due to the lack of insight into the ranking practice behind it. According to the Modernisation Directive (No. 11a Annex I UCP Directive nF), "purchased" ranking positions without a clear advertising label are always prohibited. Furthermore, according to Art 7 (6) UCPD nF, providers must disclose whether and, if so, how they check whether ratings come from "real buyers". However, such transparency obligations alone are not sufficient.

**What is missing:** platforms that allow ratings from buyers **should actually have to take reasonable measures against purchased, fake ratings from agencies.** Operators of comparison websites would also have to prove their "independence" by observing certain "design obligations": For example, commissions should not have any effect on the comparison result. Regulatory bonds can be taken from the international standard ISO 20488/2018 (Online Consumer Reviews), which contains requirements for rating systems.

Under the following link you can find the consultation questionnaire answered by AK for information and further use:
https://www.akeuropa.eu/public-consultation-european-commission-digital-services-act.

## Contact us!


**In Vienna:**

**Frank Ey**
T +43 (0) 1 501 651 2768
frank.ey@akwien.at

**Daniela Zimmer**
T +43 (0) 1 501 651 2722
daniela.zimmer@akwien.at

**Ulrike Ginner**
T +43 (0) 1 501 651 2142
ulrike.ginner@akwien.at

**In Brussels:**

**Alice Wagner**
T +32 (0) 2 230 62 54
alice.wagner@akwien.at

**Bundesarbeitskammer Österreich**
Prinz-Eugen-Straße 20-22
1040 Vienna, Austria
T +43 (0) 1 501 65-0

www.arbeiterkammer.at

**AK EUROPA**
Permanent Representation of Austria to the EU
Avenue de Cortenbergh 30
1040 Brussels, Belgium
T +32 (0) 2 230 62 54

www.akeuropa.eu


## About us

The Austrian Federal Chamber of Labour (AK) is by law representing the interests of about 3.8 million employees and consumers in Austria. It acts for the interests of its members in fields of social-, educational-, economical-, and consumer issues both on the national and on the EU-level in Brussels. Furthermore the Austrian Federal Chamber of Labour is a part of the Austrian social partnership. The Austrian Federal Chamber of Labour is registered at the EU Transparency Register under the number 23869471911-54.

The main objectivs of the 1991 established AK EUROPA Office in Brussels are the representation of AK vis-à-vis the European Institutions and interest groups, the monitoring of EU policies and to transfer relevant Inforamtion from Brussels to Austria, as well as to lobby the in Austria developed expertise and positions of the Austrian Federal Chamber of Labour in Brussels.