EPICENTER .WORKS
for digital rights

Hate on the Net & Platform Regulation

Will the European Digital Service Act replace the Austrian Communications Platforms Act?

Table of contents

Overview 1
The roots of the Digital Service Act 2
Essentials of the Communications Platforms Act (KoPlg) 2
Essentials of the Digital Service Act (DSA) 3
Differences between DSA and KoPlg 3
Reporting illegal content 3
The reporting procedure in the KoPlg 4
The notification procedure in the DSA 4
To which online platforms do these laws apply? 5
Scope of application of the KoPlg 5
Which institutions are responsible for supervision and how are sanctions imposed? 6
What are the transparency obligations? 8
Reporting obligations of supervisory authorities 8
Does the KoPlg require a mere amendment or is it obsolete with the introduction of the DSA? 9
Conclusion 10

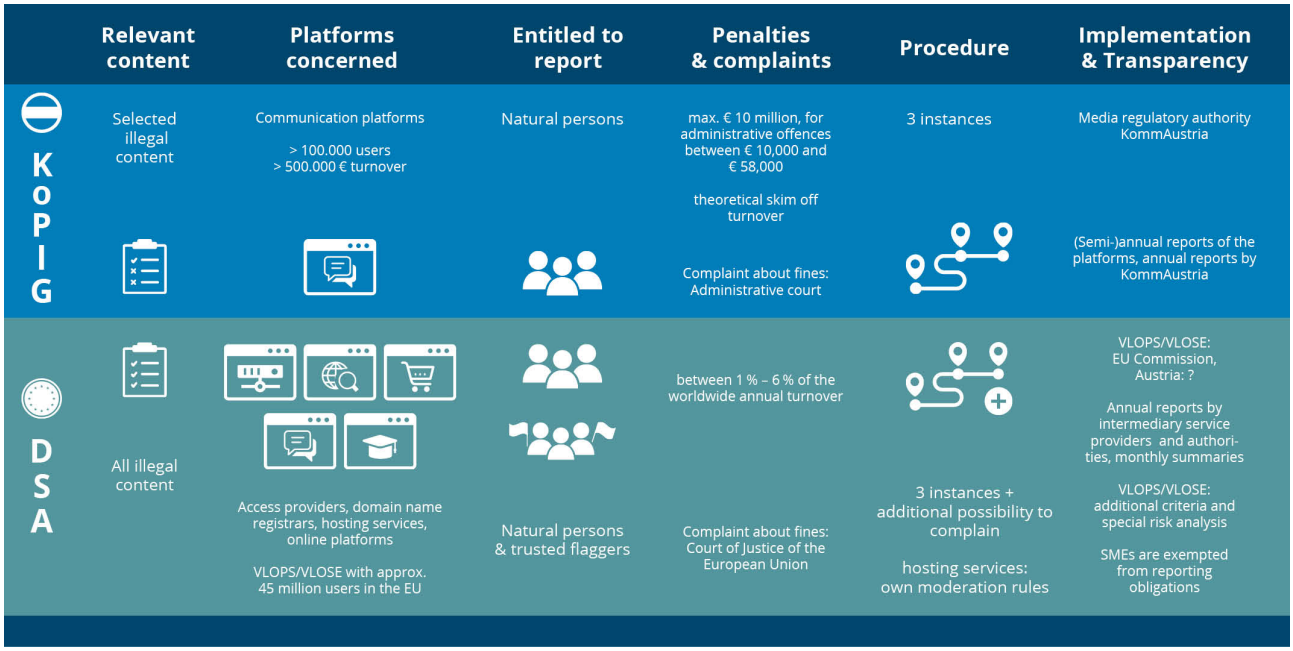
OVERVIEW

In 2020, there was a lively debate in Austria on the topic of hate on the net. The reason has been more and more insults, misinformation and even threats were spreading on communication platforms on the internet. In particular, these arose from racist, xenophobic, misogynistic and homophobic motives. The annual ZARA-Rassismus-Report confirmed this development. Online violence also has social, psychological, emotional and psychosomatic consequences for those affected. As part of the solution to combat "hate on the net", the federal government saw a need to pass a law, the Austrian Communications Platforms Act (Kommunikationsplattformen-Gesetz – KoPlg), as part of its government program 2020 - 2024. The aim was to counteract hate and violence on the net, as social media providers often do not adequately or promptly comply with existing obligations to remove illegal content and only check on the basis of their own community guidelines and not on the basis of the relevant criminal provisions. Currently, different laws exist for these services in the Member States. The example of the Austrian KoPlg can be used to show how smaller companies are hindered when they want to grow their business and expand across the EU. In addition, there is a different level of protection for European citizens.

After Austria had taken the lead with the KoPlg in the course of the hate on the net debate, an agreement has now been reached at EU level, the so-called "Digital Services Act". Now it raises the question how the two laws relate to each other, which is more comprehensive and where are weak points or is the KoPlg even outdated? The government must entrust the concerned authorities with the implementation of the more modern DSA, in order to have a positive effect in Austria. To hand

over all of the responsibility to the media regulatory authority KommAustria, which has ties to the turquoise ÖVP, (Austrian People's Party), would be a mistake.

The KoPlg has so far been rather rudimentary and has disregarded some aspects or placed an excessive burden on smaller companies. epicenter.works already submitted a statement in the review procedure for the Communications Platforms Act, which is modeled on the German Network Enforcement Act (Netzwerkdurchsetzungsgesetz – NetzDG), on 13 October 2020. However, the DSA regulates the topic more fundamentally and takes up some points of criticism that were raised against the KoPlg. Parts of the KoPlG may also be useful in the future, but there is an urgent need to reform those parts that contradict EU law or make it unnecessarily complicated. This is especially true for the areas of responsibility of the national supervisory authority, reporting obligations or activity reports and the complaints mechanism. In the following, both laws are compared and the need for change is outlined.



THE ROOTS OF THE DIGITAL SERVICE ACT

The underlying legal framework for the provision of digital services in the EU is the e-commerce directive adopted in 2000, which has been implemented by national laws in the Member States. After more than 20 years, the legal framework is now being adapted to digital progress. Online platforms bring benefits to consumers and facilitate innovation as well as cross-border trade. However, these platforms are also abused for the distribution of illegal content or the sale of illegal goods. Large service providers have become quasi-public spaces for information exchange and online trade. This also entails particular risks for user rights. Moreover, the original e-commerce directive did not lay down rules for cooperation between public authorities.

The Digital Services Act builds on the original e-commerce directive while addressing the specific challenges faced by online intermediaries. Long before the legislative proposal to regulate online

platforms at the European level was released, epicenter.works proposed platform regulation at platformregulation.eu[1] that took into account fundamental rights.

Essentials of the Communications Platforms Act (KoPlg)

The KoPlg should help to create an effective and transparent notification procedure for dealing with illegal content and should be easily and permanently accessible. The KoPlg is applicable to domestic and foreign service providers[2], with the exception of very small providers, online marketplaces and online encyclopedias or similar knowledge brokers. Furthermore, the KoPlg contains an obligation to review specific reports and, under certain circumstances, an obligation to delete them immediately, whereby users must be informed of the deletion. In the case of complaints about a specific content decision, a review option must be provided by the platform to the person posting the offending content and the person reporting the content.

Essentials of the Digital Service Act (DSA)

The Digital Services Act regulates the obligations of digital services that act as intermediaries ("Intermediary Service Providers") and enable consumers to access goods, services and content. These intermediaries include: Domain Name Registrars (DNS), mere conduit services[3], i.e. Internet Service Providers (ISPs), hosting services[4], e.g. cloud service providers, online marketplaces, social media, app stores and caching services[5], e.g. CloudFlare.

Online platforms[6] include social networks, online marketplaces, app stores, online travel and accommodation websites, content sharing websites e.g. Facebook and collaborative economy platforms. Classic search engines include, for example, DuckDuckGo or Google.

Unlawful content[7] that can appear on these platforms, can be reported under the new regulation in the DSA if it is disseminated to the public[8]. Such content concerns hate postings, which are xenophobic or misogynistic, homophobic or fundamentally offensive and can thus be prosecuted. E-mail or private messaging services are excluded from these platforms and search engines, as well as micro or small enterprises (SMEs). However, the DSA specifically targets very large online platforms and very large search engines, with a number of additional strict requirements applying to the providers of such platforms.

1 https://platformregulation.eu/

2 According to § 2 no. 3 KoPlg, service providers are natural or legal persons who offer a communication platform. Pursuant to § 3 no. 4 KoPlg, a communications platform is in turn an information society service which primarily enables communications by means of mass dissemination.

3 Art. 2 lit. f (i) in conjunction with Art. 3 DSA: A mere conduit service is the transmission of information provided by a recipient of the service in a communications network or the provision of access to a communications network, e.g. internet service providers.

4 Art. 2 lit. f (iii) in conjunction with Art. 5 DSA: Hosting services are those services that store information provided at the request of the recipient, e.g. cloud service providers, online marketplaces, social media, app stores.

5 Art. 2 lit. f (ii) in conjunction with Art. 4 DSA: A caching service serves the more efficient transmission of requested information in a communication network to other recipients. This information is provided by a recipient of the service and is automatically temporarily stored.

6 Art. 2 lit. h DSA: Online platforms are those that publicly disseminate the information of users.

7 Art. 2 lit. g DSA: Content is unlawful if the information, as such or in connection with an activity, including the sale of products or the provision of services, infringes Union law or the law of a Member State.

8 Art. 2 lit. i DSA: Dissemination to the public means information made available to an unlimited number of persons. However, this does not include dissemination in closed groups composed of a limited number of people, such as e-mail or private messaging services, therefore these types of services are not considered online platforms in the sense of the DSA.

An online platform is considered a very large online platform (VLOPS) or a very large search engine (VLOSE) if the number of average monthly users is 10% or more of total EU consumers (currently 45 million people).[9] The European Commission explicitly identifies[10] which entities are very large online platforms or very large search engines and is the competent supervisory authority for them.

DIFFERENCES BETWEEN DSA AND KOPLG

Reporting illegal content

If someone sees an offensive post, it can be reported, as well as the associated accounts that posted it. This is usually done via a button near the post or the posting account.

The reporting procedure in the KoPlg

In Austria, the legal basis was established in 2020 with the Communications Platforms Act (KoPlg).[11] The reporting function must be easy to find, permanently available and easy to use for the user.

A post should be removed within 24 hours if laypersons can easily classify content as illegal. In more difficult cases, a detailed examination and a decision must be made within seven days.[12] In the case of a removal or blocking, evidence for a possible prosecution needs to be kept for up to 10 weeks. In addition, the person concerned must be informed of the outcome of the review, both the person who posted the content and the person who reported it as potentially unlawful. This information must contain essential reasons for the platform's decision and can be objected to by both parties involved with the platform in a review procedure. Should this result in an unsatisfactory outcome, the decision can be reviewed by means of a complaint procedure at the RTR.

In principle, the KoPlg provides for an internal review possibility regarding the reporting procedure. Thus, persons whose posts are affected and also those who report the post can have the procedure reviewed. If the review procedure by the communications platform is not satisfactory, the affected group of persons can turn to the competent authority, i.e. in principle the national supervisory authority, in Austria the Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH).[13] The latter then reviews the reporting procedure for inadequacies and is supposed to propose an amicable solution.[14] If there is a complaint against decisions on fines, recourse can be made to the Administrative Court.

This clearly shows that the DSA concretizes the regulations of the KoPlg, not only natural persons can file complaints and the competence of the authorities differs depending on the size of the service. Likewise, the out-of-court dispute resolution process must be taken into account in a possible amendment of the KoPlg.

9 Art. 25 in conjunction with 33a DSA.
10 Art. 25 (4) (2) DSA, Art. 33a (1) in conjunction with Art. 25 (4) DSA.
11 § 3 KoPlg.
12 § 3 KoPlg.
13 § 7 KoPlg.
14 § 7 KoPlg.

The notification procedure in the DSA

The Digital Service Act, which will apply from 2024, is an EU regulation, i.e. it applies directly in all EU Member States without the need for a national law to implement it. Regulations of the KoPlg that conflict with the DSA will no longer be applied.

The DSA also contains regulations on reporting procedures, according to which providers of hosting services must provide a mechanism so that illegal content can be reported.[15] At the same time, providers must provide a so-called *Statement of Reason*, i.e. a reason why which information has been deleted. This is similar to the current notification of the result of the review under the KoPlg.

New is that not only individuals can report hate postings, but also other bodies and so-called "trusted flaggers". These are recognized civil organizations such as ZARA or investigative authorities. These already existed on some large platforms, but without a legal basis. They can submit an application to the Digital Service Coordinator of the Member State in which they are based. These notifications will be treated preferentially, as they will be reviewed first. Nevertheless, the review of the notification must follow the same procedure as the notification by individuals. Only on the basis of the authority of the Trusted Flaggers, a post may not simply be removed - without further review.

Platforms are not only required to keep evidence, but are also subject to a reporting obligation for content relevant to criminal law. However, there are no general monitoring or active investigation obligations, e.g. to check all posts for possible offensive content or hate messages by means of an algorithm or own staff..[16] This also applies to messaging. If all chats and posts are constantly checked for illegal content, users are no longer free to decide what they write or post. In addition, measures against abuse of online platforms must be implemented, e.g. an account that posts illegal content several times can be temporarily blocked.[17]

According to the new regulations, "dark patterns" are also prohibited. Online platform providers may not design, organize or operate their online interfaces in such a way that the users of their services are deceived or manipulated or their freedom of choice is impaired.

Ultimately, the reporting procedure in the DSA has been refined, there are reporting possibilities for more people or organizations and a graduated review mechanism with information obligations. In addition, there is an obligation to take action in the case of criminal offenses. However, a general algorithmic or staff review of all comments is not endorsed.

The DSA provides for an internal complaints procedure, as well as an external one, a so-called Out-Of Court Dispute Mechanism. This out-of-court procedure involves certified bodies. Specifically, recipients of the service, i.e. individuals or other bodies who have submitted reports and are the addressees of the provider's decision,[18] can present their complaints and have decisions reviewed.

In addition, recipients of the service have the right to lodge a complaint.[19] A complaint against the switching service can be lodged with the Digital Services Coordinator of the Member State in which the recipient is domiciled if the DSA has been breached.

15 Art. 14 DSA.
16 Art. 7 DSA.
17 Art. 20 DSA.
18 Art. 17 (1) DSA.
19 Art. 43 DSA.

To which online platforms do these laws apply?

Scope of application of the KoPlg

The scope of application of the KoPlg differs from the DSA. Within the broad scope of application, the KoPlg already covers communication platforms with 100,000 or more users or a turnover of €500,000 in Austria. Service providers of video sharing platforms as well as online marketplaces, non-profit online encyclopedias or educational and learning platforms as well as media companies offering journalistic content are not or were not included.

Scope of the DSA

The DSA, on the other hand, applies to a wide range of online intermediaries, which include, among others, internet service providers, but also operators of cloud and messaging services, marketplaces or social networks. Specific due diligence requirements apply to hosting services and in particular to online platforms, such as social networks, content sharing platforms, app stores, online marketplaces and online travel and accommodation platforms. However, so-called small and medium-sized enterprises (SMEs)[20] are exempted.

For very large online platforms and search engines, so-called Very Large Online Platforms (VLOPS) and Very Large Search Engines (VLOSE), the DSA provides for special regulations, as these large online platforms have a significant social and economic impact.

In particular, the differences in the scope of application show that the KoPlg needs to be adapted. Although the provisions of the KoPlg that conflict with the DSA are no longer applicable once the DSA enters into force, an amendment is also needed for reasons of clarification. The exemptions for SMEs must be made clear, as well as the extended scope of application to online marketplaces and the like. In addition, the distribution of competences between the EU Commission and national authorities is changing with regard to so-called VLOPS and VLOSE. This must be taken into consideration in the KoPlg, as the KoPlg otherwise contains regulations that violate the DSA.

Which institutions are responsible for supervision and how are sanctions imposed?

At the moment, the KoPlg provides that KommAustria and its associated part of RTR are the competent authority.[21] They are financed by contributions from the service providers, measured in terms of their domestic revenues.[22] If a complaint is received about a service provider and there is a breach of duty, the supervisory authority initiates supervisory proceedings and orders the service provider to remedy the breach of duty by means of a regulatory decision. If the service provider does not comply, a fine will be imposed. If the service provider is domiciled abroad, it is also possible to collect the fine by having the supervisory authority collect claims that the service provider has against other companies in Austria.[23]

In principle, under the new DSA, it is up to the Member States to designate the competent authorities in their country. However, the DSA also affects data protection issues and in any case the data protection authority should be the competent authority to implement the DSA. The DSA also concerns some telecoms issues, for example in relation to ISPs, or the review of T&Cs and consumer protection

20 10-250 employees, 2 Mio. - 50 Mio. € turnover respectively 43 Mio. € on the balance sheet.
21 § 8 KoPlg.
22 § 8 (3), (4) KoPlg.
23 § 6 (4) KoPlg.

issues. In this area, the Telekom-Control Commission (TKK), already has jurisdiction and a high level of expertise. To avoid contradictory decisions in these areas, the DPA and the TKK - with its associated part of the RTR - should each be the competent authority for these issues. If KommAustria had the final decision on all these issues, it would not only be contrary to the high level of expertise in the other specialist authorities, it would also lead to a de facto devaluation of the DPA and the TKK in their respective areas and ultimately to a fragmentation in questions of telecom, data protection and consumer protection law.

Separate from this issue is the need to clarify which authorities will be designated as national Digital Service Officers. Similar to a data protection authority, a national Digital Service Officer shall cooperate at national or European level and ensure coherence.[24] At European level, a European Board for Digital Services will be established, which will form an independent group of Digital Service Coordinators. This board will contribute to and advise the Digital Services Coordinators and the European Commission on the harmonized application of the DSA and efficient cooperation as well as on guidelines and analyses of the European Commission. Moreover, it will support the supervision of VLOPS and VLOSE.

The Member States are responsible for the Intermediary Service Provider, which has its head office in the respective Member State, exclusively with regard to supervision and enforcement of supervisory decisions in case of infringements. By way of derogation, the European Commission is responsible for VLOPS and VLOSE.[25]

In enforcing the rules of the DSA, the European Commission has powers to gather information, conduct interviews and inspections of VLOPS and VLOSE, also upon request of a Digital Service Coordinator of a Member State. In this context, it is critical that the EU Commission is not an independent authority and that it is therefore legally difficult to entrust it with law enforcement tasks.

At the same time, the Member States are given certain regulatory freedoms in the area of sanctions. The DSA only provides for an upper limit, which Austria lags far behind.[26] Currently, the KoPlg provides for fines for various infringements.[27] These amount, for instance, to € 1 million for failure to appoint a responsible officer or € 10 million if no notification procedure is provided or no measures for blocking and deletion are taken. In determining the amount[28], the financial strength of the service provider is also taken into account, as well as the extent and duration and the number of registered users. Further administrative offenses are punished with € 10,000 - 58,000. However, this is well below the possibility of the DSA and is not sufficiently deterrent. As relatively small service providers also fall under the KoPlg, these penalties bring them to the brink of ruin. Large companies like Facebook and Co. do not see this as a serious penalty.

Sanctions should rather be based on the General Data Protection Regulation. This orientation is already clearly visible in the DSA:

The Member States can determine the amount of the fines, with the amount varying between 1 %-6 % of the global annual turnover of the previous year depending on the violation.[29] The maximum of a repeated sanction is supposed to be 5 % of the average daily global annual turnover. In addition, the

24 Art. 39 ff. DSA.
25 Art. 44a (1a), (1b) DSA.
26 Art. 42, 59 DSA.
27 § 10 KoPlg
28 § 10 (3) KoPlg.
29 Art. 42 (1), (3) DSA.

European Commission itself can impose fines of up to 6 % of the worldwide annual turnover on VLOPS and VLOSE.

Sanctions in the DSA include not deleting hate posts, or deleting too much and not having guidelines for deletion in place, or reporting posts for deletion is too burdensome, not naming responsible parties, not complying with reporting obligations or not releasing information (in a timely manner). In addition, VLOPS and VLOSE must have a so-called "compliance function", i.e. a team in the company which, like the data protection officer, has a possibility of enforcement and can act independently of other departments if regulations of the DSA are not complied with.

What is new, however, is the possibility of compensation for persons affected by hate postings. In the DSA, there is the possibility to demand redress.[29]

Particularly in the area of supervision, a new type of division of competences between the EU and Member States is becoming apparent, as well as the introduction of new institutions such as the Digital Service Officer at national level. The KoPlg must take these changes into account and consider them in an amendment. There is also an immense need for adaptation in the area of sanctions. Although the DSA only provides for a cap, there is still a lot of room for improvement in the KoPlg. In addition, the distribution of competences with the EU Commission must be taken into account with regard to sanctions.

What are the transparency obligations?

The KoPlg provides for a reporting obligation regarding the number of reported and deleted posts, among other things. In principle, this should be done annually, and in the case of more than 1 million users, every six months.

However, the DSA exempts SMEs from reporting obligations to a certain extent.[30] Otherwise, Intermediary Service Providers must submit an annual report on reported posts and any moderation of content.[31] In addition, there is a transparency reporting obligation for providers of online platforms that is more extensive than that of the KoPlg.[32]

Furthermore, online marketplaces must implement a know-your-customer (KYC) programme[34] so that traders can only use the services if they disclose enough information about their company

An additional extended transparency obligation applies to very large platforms and search engines, the VLOPS and VLOSE.[35] They must annually conduct a special risk analysis regarding algorithms and other functions in the system, also the design of recommendation systems and other elements must be examined.[36]

Between KoPlg and DSA there is a wide divergence between the reporting and transparency obligations. Since the DSA also provides for special obligations for VLOPS and VLOSE and thus

29 Art. 43a DSA.
30 Art. 16 DSA.
31 Art. 13 DSA.
32 Art. 23 DSA.
34 This means that the online marketplace must be able to identify the trader with official documents; the transmitted data includes in particular: especially on products, contact, identification and payment data of the trader.
35 Art. 33 DSA.
36 Art. 27 DSA.

differentiates between company size, the KoPlg must be amended in this respect. In particular, the limit for the size of the enterprise above which various obligations exist must be adjusted.

Reporting obligations of supervisory authorities

Supervisory authorities also have a reporting obligation. For Digital Service Coordinators, this consists of disclosing a report to the public, the Commission and the European Board of Digital Service Coordinators on the number of complaints and orders received, as well as their subject matter.[37]

According to the KoPlg, the appeal body has to prepare an annual report on the pending cases,[38] which has to be published in the context of the activity report. Monthly summaries of the number, type and content of complaints are made available to the supervisory authority, i.e. the Communications Authority Austria, which is supported by RTR.

DOES THE KOPLG REQUIRE A MERE AMENDMENT OR IS IT OBSOLETE WITH THE INTRODUCTION OF THE DSA?

In view of the points mentioned above, in which the KoPlg and the DSA contradict each other and the DSA provides possibilities for regulations by the Member States, an amendment of the KoPlg by the responsible Minister Karoline Edtstadler is absolutely necessary. Although the DSA is a regulation that applies directly in the Member States, it also contains provisions that give the Member States room for discretion. Since Austria already disposes of the KoPlg, this leeway should be used.

The tension between the KoPlg and the DSA is mainly in the scope of application, i.e. the DSA is much more specific and explicitly exempts SMEs from strict (reporting) obligations so that they are not unduly affected, whereas the KoPlg already makes communication platforms liable when reaching 100,000 users or €500,000 turnover in Austria. Thus, this part of the KoPlg is no longer applicable with the entry into force of the DSA. At the same time, the DSA expands the scope of application by explicitly including online marketplaces in the obligation, whereas the KoPlg just excludes them. In this respect, the KoPlg also becomes obsolete.

With regard to sanctions, the Member States have a margin of appreciation, which Austria should also use in order to create an increased incentive for companies to comply with the regulations. Therefore, the law only requires an adjustment.

In principle, reference can be made to the DSA regarding the reporting obligations, which regulates these depending on the platform. The supervisory fees must also be newly regulated in the KoPlg, since the European Commission itself collects supervisory fees from VLOPS and VLOSE.

Finally, it can be said that the DSA approaches the challenges of hate speech on the net in a better way than the KoPlg, namely in a European, international way that includes the structures of large corporations as well as the need for coherent cooperation at the European level. In particular with

37 Art. 44 DSA.

38 § 7 (3) KoPlg in conjunction with § 19 (2) Austrian Communication Act (KommAustria-Gesetzes – KOG).

regard to so-called VLOPS and VLOSE, for which the European Commission itself is primarily responsible. In order to give structure to the whole issue, a European Board for Digital Services will be set up, similar to the European Data Protection Board. This will create a place of exchange for the national supervisory authorities and at the same time a European advisory body for the most diverse, also international issues.

At the same time, this means that there is a need to amend the KoPlg, as it must be stipulated that the national supervisory authority, currently KommAustria, which is supported by RTR, receives additional tasks regarding European cooperation and reporting obligations or activity reports. The complaints mechanism, which will be set up with the help of certified out-of-court bodies, must also be taken into account in the KoPlg. With regard to the areas of responsibility, reference is made to the specific distribution of competences between the European Commission and national supervisory authorities with regard to VLOPS and VLOSE.

In addition, VLOPS are required to have a so-called "compliance function", not just a mere officer who has no authority to enforce the regulations of the DSA. In the EU, a legal representative must be appointed if there is no registered office in a Member State; this representative can be held liable for breaches of duty.[39] The KoPlg also provided for the appointment of a responsible person, also for companies not based in Austria, but which have a large number of users. The non-appointment of a responsible person is not sanctioned strongly enough for financially strong and large service providers with a maximum of € 10 million. Again, the personal liability of a responsible representative or agent for service of up to € 10,000 for not making his/her contact details immediately accessible is set relatively high.[40]

For this purpose, the KoPlG has chosen the special path of making the authorized representative of an online platform liable himself/herself if the company does not comply with the rules. In practice, this was solved in Austria with very well-paid law firms. Another Austrian curiosity of the KoPlG was the skimming off of revenues of online platforms if they did not comply with the KoPlG. Both regulations are questionable, have demonstrably not helped - Telegram refuses to implement the KoPlG - and should be repealed.

CONCLUSION

Despite some shortcomings and missed opportunities, the DSA is a big step in the direction of a fairer internet for all. Simply because of the horizontal application to all potentially illegal content, the better enforcement of harmonized EU rules and the special attention to the major platforms, one should not shed a tear for the KoPlG. This means for the federal government and especially the responsible minister Karoline Edtstadler that the KoPlG must be reformed. In January/February 2023, a draft assessment of the implementation of the DSA in Austria is expected under the auspices of the Federal Chancellery.

In any case, legal adjustments are needed in Austria in order to designate the Digital Service Officer at the national level. In this context, the data protection authority should be the competent authority in questions of data protection and the TKK should be the competent authority in questions of general terms and conditions reviews, telecom issues and consumer protection, or at least decisions in these

39 Art. 11 DSA.
40 § 10 (4), (5) KoPlg.

areas should be made in agreement with these authorities. However, the KoPlG must also be reformed because some of its provisions are clearly in conflict with the DSA and EU law takes precedence over national law.