Do the New European Rules on Digital Services Effectively Ensure Human Rights on Platforms? Assessment model for states

Müller, Martin; Rachinger, Felicitas; Vural, Meryem; Kettemann, Matthias C.

Erstveröffentlichung / Primary Publication
Arbeitspapier / working paper

Empfohlene Zitierung / Suggested Citation:
Müller, M., Rachinger, F., Vural, M., & Kettemann, M. C. (2024). *Do the New European Rules on Digital Services Effectively Ensure Human Rights on Platforms? Assessment model for states.* (GDHRNet Working Paper, 2). Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI). https://doi.org/10.21241/ssoar.96409

MARTIN MÜLLER, FELICITAS RACHINGER, MERYEM VURAL & MATTHIAS C. KETTEMANN

Do the New European Rules on Digital Services Effectively Ensure Human Rights on Platforms?

Assessment model for states

Milestone 2 · Global Digital Human Rights Network 2024

„All human beings are born free and equal in dignity and rights.“

Art. 1, sentence 1, Universal Declaration of Human Rights (1948),

Do the New European Rules on Digital Services Effectively Ensure Human Rights on Platforms?

Assessment model for states

by Martin Müller, Felicitas Rachinger, Meryem Vural & Matthias C. Kettemann
(UNIVERSITY OF INNSBRUCK & LEIBNIZ INSTITUTE FOR MEDIA RESEARCH | HANS-BREDOW-INSTITUT, HAMBURG)

Cite as: Müller, Martin; Rachinger, Felicitas; Vural, Meryem; & Kettemann, Matthias C. (2024). Do the New European Rules on Digital Services Effectively Ensure Human Rights on Platforms. Assessment Model for States. Hamburg: Verlag Hans-Bredow-Institut. https://doi.org/10.21241/ssoar.96409

GDHRNet is funded as EU COST Action – CA19143 – by the European Union.

Publisher: Leibniz Institut für Medienforschung | Hans-Bredow-Institut (HBI)
Rothenbaumchaussee 36, 20148 Hamburg
Tel. (+49 40) 45 02 17-0, info@leibniz-hbi.de, www.leibniz-hbi.de

Executive Summary

- Nine GDHRNet members participated in the survey. Of these participants, seven report on EU member states (Austria, Cyprus, Czechia, Finland, Germany, Italy, Portugal), and two on non-EU member states (Moldova, and Serbia).
- A Digital Services Coordinator (DSC) – which is the supervisory authority to be established under the DSA – has been appointed in Austria, Czechia, Cyprus, Finland, Germany, Italy and Portugal.
- Where a DSC has been designated, the state reports indicate that existing authorities overseeing telecommunication and/or media authorities have been chosen to function as DSC.
- Most reports show that the national DSCs are sufficiently equipped, but the report on Czechia indicates a lack of staff, while the report on Cyprus indicates limited financial resources.
- DSCs are granted sufficient power to request data from service providers. The reports show that national legislation is closely oriented on the requirements the DSA sets out.
- Under the DSA, sanctions are to be imposed by the member states in cases of DSA infringements by service providers. In those states where such legislation is in place, it closely follows DSA requirements (especially regarding the maximum amount).
- Reports on Finland, Italy, and Austria show that DSCs are required to cooperate with other authorities within their state, but also with other national DSCs. For example, the Austrian DSC is required to regularly interact and exchange their opinions and experiences regarding certain topics with other DSCs.

Contributors

Country	Name(s)
Austria/Germany	Martin Müller, Felicitas Rachinger, Meryem Vural
Cyprus	Philippe Jougleux, Constantinos Kouroupis
Czechia	Federica Cristani
Finland	Jukka Viljanen, Riku Neuvonen
Italy	Federico Costantini, Andrea De Coppi
Moldova	Elina Benea-Popușoi, Vitalie Ursachi
Portugal	Alexandre Dias Pereira
Serbia	Jelena Simic

Table of Contents

Executive Summary **4**

Contributors **5**

Table of Contents **6**

Introduction and Methodology **7**

Foundations for an Assessment Model **8**

Questionnaire and summary of responses **10**

How will national law be adapted to the DSA? 10

What does this supervisory structure look like? 11

How will the DSC have access to the data of intermediary services? 14

What are the sanctions to be imposed by the Member States in case of infringements of the DSA by the intermediary services providers? 15

How is cooperation between national authorities structured? Are there any guidelines on cooperation with other national DSCs? If yes, how is such cooperation structured? 16

What obligations exist for companies not covered by the DSA? 16

What are the rules regarding the evaluation of systemic risks (if complementary to those in the DSA)? 17

How is the integration of civil society structured? 17

Is there an advisory board to raise the quality of the democratic feedback of the development of rules and practices of the platforms? 17

EU COST Action – CA19143: Global Digital Human Rights Network **18**

Introduction and Methodology

The GDHRNet (Global Digital Human Rights Network) is dedicated to the investigation of theoretical and practical challenges of the protection of human rights in the digital context. Platforms in particular face the challenge of organizing their services in a way that respects and protects the fundamental rights of their users.

Over recent years, the European legislator has introduced a comprehensive range of legal instruments, including the E-Commerce Directive[1], the General Data Protection Regulation (GDPR)[2], as well as the Digital Services Act (DSA)[3] and the Digital Markets Act (DMA)[4], to effectively regulate the EU Digital Single Market. The DSA in particular aims to ensure *"a safe, predictable and trustworthy online environment"*[5] and therefore stipulates in its Article 14 (4) the obligations for platforms to take the fundamental rights of their users into account.

In light of the above-mentioned this study examines the obligations for platforms in 9 GDHRNet-member states, including 7 EU-member states, to ensure the protection of fundamental rights. Based on the responses to a questionnaire by country rapporteurs, and the analysis conducted by the editors, this study has two outcomes which are at the same time the Milestones of the GDHRNet for 2024: The development of guidelines for platforms to offer and carry out their online activities in accordance with fundamental rights (Milestone 1) and secondly, the creation of an assessment model to evaluate the compliance of platform services regarding the protection of human rights (Milestone 2).

This document entails part 2 of the study (Assessment model for states). The aim of the study was to develop the foundations of an assessment model for assessing the compliance of online companies regarding human rights protection obligations. An executive summary recapitulates the main results of the study (2). The findings of the study have been built into the foundations of an assessment model (3). The study builds upon a questionnaire focusing on national platform oversight structures that has been sent out to GDHRNet members. To each question, there is a summary entailing the relevant information provided by GDHRNet members (4). The scope of the study is limited to the GDHRNet members' responses to the questionnaire. No additional information has been added.

---

[1] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce'), OJEU 2000 L178/1.

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJEU 2016 L119/1.

3 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJEU 2022 L277/1.

4 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJEU 2022 L265/1.

5 Recital 12, DSA, L 277/4.

Foundations for an Assessment Model

For **Milestone 2 (Assessment Model)** GDHRNet members develop the foundations of an assessment model for assessing the compliance of online companies regarding human rights protection obligations. In the EU, national authorities are required to assess online companies regarding obligations under the Digital Services Act: The DSA contains specific regulatory mandates directed at Member States. Accordingly, a Digital Services Coordinator (DSC) is to be established in each Member State as a new supervisory authority, which is to receive complaints from users from the respective Member State and ensure access to the data of the intermediary services.

The assessment model is built upon a questionnaire which allowed to gather information on the assessment of online companies by these national authorities (DSCs). The analysis of the reports on the questionnaire by GDHRNet members allowed to compile this list of requirements and considerations for a human rights-based assessment of online companies:

1. Designation of an already existing national authority in the field of media and/or telecommunication regulation.

The report showed that member states rely on already existing authorities to assess online companies. This allows them to draw on preexisting experience and knowledge in the field of media and/or telecommunications as well as preexisting structures within the authority.

2. Guarantees of independence of the national authority, including the allocation of sufficient resources.

While there were no specific reports about the (lack of) independence of any national authority, the reports showed a common concern about guarantees of independence, proving the independence of national authorities essential for human rights-based assessment of online companies. This goes hand-in-hand with the allocation of sufficient technical, financial, and human resources, which are a prerequisite for the performance of any assessment.

3. Coordination with other national authorities.

Under the DSA, many GDHRNet member states are required to designate a DSC. This leads to a lot of experience spread across different authorities. Coordination between these authorities is essential in order to share this information and knowledge. This coordination should be legally established.

4. Involvement of civil society

The assessment of online companies should be carried out with the involvement of civil society. This allows national authorities to draw on the valuable experiences and perspectives of civil society organizations. For example, such involvement can be carried out through an advisory board.

5. Development of risk assessment mechanism and an information security strategy

The report showed that various GDHRnet member states have implemented cybersecurity frameworks and risk assessment mechanisms to address threats from digital platforms and protect national security. These efforts are complemented by EU-wide regulations like the DSA or the NIS 2 Directive and crisis management structures designed to enhance the resilience of digital services and mitigate cyber risks. The national regulatory bodies of the GDHRnet member states should cooperate and develop guidelines in relation to specific risks.

6. Access to data

When assessing online companies, access to data is crucial. Only if sufficient information about the rules and processes of online companies is available, an assessment can be performed successfully. Access to data shall be legally established.

7. Transparency about content moderation and advertising

Besides data access, transparency about content moderation processes and advertising is essential to enable an effective evaluation of the compliance of online companies regarding human rights obligations. The report indicates that a range of GDHRNet member states, also non EU-members, have already implemented transparency requirements for platforms into their legal framework.

8. Cooperation with Trusted Flaggers

Under the DSA, platforms are allowed to cooperate with trusted flaggers. The Trusted flagger status is granted by the DSC of the member state and the status is designated to organizations which demonstrate expertise in handling illegal content and operate with diligence and objectivity. Platforms benefit from the cooperation with trusted flaggers and therefore can address illegal content more effectively. Platform shall collaborate with trusted entities under legal frameworks to address harmful content.

Questionnaire and summary of responses

How will national law be adapted to the DSA?

Will there be legislative amendments related to the DSA?

Austria was the first European country to pass a law implementing the DSA, which is called DSA-Begleitgesetz (DSA-BegG)[6], and has resulted in several changes to the Austrian law. The national telecommunications authority KommAustria has been designated as national DSC, which required a legislative amendment in the KommAustria-Gesetz[7]. A new Act, the Koordinator-für-digitale-Dienste-Gesetz – KDD-G[8] was enacted and concerns powers and obligations of the national DSC and at the same the KoPl-G is repealed.[9]

In Germany, the DSA will be implemented through the *Digitale-Dienste-Gesetz* (DDG)[10], which has been passed by the *Bundestag* recently.[11] The following information is based on the latest public draft of the Digitale-Dienste-Gesetz: Part one of the DDG (Article 1-4 DDG) contains provisions on the necessary legislative amendment which must be made to adapt national law to the terminology of the DSA. Germany designated the *Bundesnetzagentur* (Federal Network Agency) as the DSC which is included in § 12 (1) DDG. Furthermore, the *Telemediengesetz* (TMG) and the most part of the NetzDG will be repealed (Article 29 and 35 DDG). Existing requirement of the NetzDG and TMG that are relevant to compliance effort will be then directly enforced by the DSA or by German federal law in form of the DDG. In addition to the Bundesnetzagentur as the DSC in Germany, special responsibilities will be created for the Federal Agency for the Protection of Children and Young Persons in the Media. An office for the enforcement of children's right in digital services will be established at the Federal Agency for the Protection of Children and Young Persons in the Media, based in Bonn (§ 12 (2) DSA). The main work of the agency will be on the enforcement of Article 14 (3) and Article 28 (1) DSA. Furthermore, the Federal Commissioner for Data Protection and Freedom of Information will be responsible for the enforcement of Article 26 (3) and Article 28 (2), (3)

6 Bundesgesetz, mit dem das Koordinator-für-digitale-Dienste-Gesetz erlassen und das KommAustria-Gesetz, das E-Commerce-Gesetz, das Allgemeine bürgerliche Gesetzbuch, das Urheberrechtsgesetz, das Gerichtsgebührengesetz, das Mediengesetz, die Strafprozeßordnung 1975, das Staatsanwaltschaftsgesetz, das Bundesgesetz über die justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europäischen Union, das Auslieferungs- und Rechtshilfegesetz und das Telekommunikationsgesetz 2021 geändert werden (DSA-Begleitgesetz – DSA-BegG) 2309 XXVII.GP.

7 KommAustria-Gesetz (KOG) of 30. March 2001 (BGBl. I No. 6/2024).

8 Koordinator-für-digitale-Dienste-Gesetz – KDD-G of … (BGBl. I No. Xxx/2023).

9 In addition, further amendments were made in the E-Commerce-Gesetz, Urheberrechtsgesetz, Gerichtsgebührengesetz, Mediengesetz, Strafgesetzbuch 1975, Staatsanwaltschaftsgesetz, Bundesgesetz über die justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europäischen Union (EU-JZG), Auslieferungs- und Rechtshilfegesetz (ARHG) and the Telekommunikationsgesetz 2021.

10 Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG sowie zur Durchführung der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten und zur Änderung weiterer Gesetze of 15 of January 2024, 20/10031.

11 Clasen, 21. 03.2024, Bundestag adopts its DSA implementation law with one-month delay, https://www.euractiv.com/section/internet-governance/news/bundestag-adopts-its-dsa-implementation-law-with-one-month-delay/ (27.03.2024)

DSA according to Article § 12 (3) DDG. Part 8 of the DDG (Article 33) contains provisions on fines which will complement the ones in the DSA.

Like Germany, Czechia also drafted a proposal for a Digital Economy Act to adapt the national regulatory framework to the DSA.

Finland enacted the Act monitoring digital services Laki (verkonvälityspalvelujen valvonnasta) which came into force in February 2024.

Will there be administrative amendments related to the DSA?

In Finland there will be no administrative amendment besides one about the reform of the Traficoms internal sanctions committee which has been designated as DSC of Finland. For Germany and Austria see above.

Will there be any other measures by your State related to the DSA?

The reports do not indicate so.

What does this supervisory structure look like?

Has your State designated a DSC?

Among responding EU member states, all have designated a DSC and reported to the Commission, pursuant to Article 49(3) DSA.[12] However, the Commission has opened infringement procedures against six EU member states for not (properly) implementing the DSA on national level.[13] The member states have not been part of the questionnaire.

Which authority has been designated? Has the authority been newly established or is it connected to an already existing authority?

The member states have designated the following authorities:

EU member state	Designated DSC	Existing authority?	Type of authority
Austria	KommAustria (Communication Authority Austria)	Yes	Media
Cyprus	Cyprus Radiotelevision Authority	Yes	Media
Czechia	Český telekomunikační úřad (Czech Telecommunication Office	Yes	Telecommunications
Germany	Bundesnetzagentur (Federal Network Agency)	Yes	Telecommunications

[12] An overview can be found here https://digital-strategy.ec.europa.eu/en/policies/dsa-dscs; an overview including *potential* authorities in the EU and EFTA here https://www.stiftung-nv.de/en/publication/overview-digital-services-coordinators-europe.

[13] https://digital-strategy.ec.europa.eu/en/news/commission-calls-6-member-states-comply-eu-digital-services-act

Finland	TRAFICOM (Finnish Transport and Communications Agency)	Yes	Media Telecommunications
Italy	Autorità per le Garanzie nelle Comunicazioni (Communications Regulatory Authority)	Yes	Media Telecommunications
Portugal	Autoridade Nacional das Comunicações (National Regulatory Authority for Communications)	Yes	Telecommunications

Source: Homepage of the European Commission

All states reported that authorities overseeing telecommunication and/or media authorities have been designated as DSC. Finland and Germany have indicated that additional authorities in consumer and data protection as well as media regulation will likely take over parts of the DSC's responsibilities.

What role does this authority take within your broader national context?

Regulation authorities in the telecommunication sectors have been subject to an extensive legal framework on an EU level[14] which has been developed in a harmonizing manner since the late 1980s. As such, differences between them regard rather specific areas. This differs, however, to those authorities serving as media regulators as well. These work together in the European Regulators Group for Audiovisual Media Services (ERGA) but follow various member state laws when it comes to media regulation. However, Austrian *KommAustria*, Cypriot Radiotelevision Authority and Italian *Autorità per le Garanzie nelle Comunicazioni* have held various media regulation responsibilities, such as those prescribed by the AVMS directive in the past.

How is the authority structured?

The regulating authorities are structured manner similar to other executive bodies. Terms of office vary from five (Finland) to six years (Austria, Cyprus) as do appointment procedures as they are carried out by the President after a suggestion by the government (Austria) or the government (Cyprus and Finland) itself. Regarding their independence, the authorities have to follow the detailed jurisprudence of the CJEU which ruled several times on the question.[15]

Is the authority equipped to perform its tasks in an impartial, transparent and timely manner?

From responding counties, Czechia noted that its authority lacks staff to perform the tasks prescribed by the DSA. As Czechia hosts a Very Large Online Platform, this might lead to difficulties in the joint enforcement with the Commission.

[14] Cf. Savin, „EU Telecommunications Law", pp. xv-xiii who lists 26 different regulations and directives in force as of 1 January 2018.

15 Most recent CJEU, Judgement of 2 September 2021, C-718/18 (Commission v Germany) EU:C:2021:662.

Does the authority have the necessary resources to carry out its tasks (including sufficient technical, financial and human resources to adequately supervise all providers of intermediary services falling within their competence)?

As noted above, there were staff issues registered for Czechia. Moreover, Cyprus reported financial difficulties for its authority. Other states have indicated that staffing as well as limited financial resources for regulatory authorities in general might hamper effective enforcement for the DSA also.

Does the authority have sufficient autonomy in managing its budget within the budget's overall limits?

There have not been registered any issues in that regard from responding countries.

Is the authority set to work completely independent? Is there any danger of external influence?

None of the responding countries reported any DSA-specific issues. As all countries follow government approval of the directorial staff at some point as well as financial resources, it was noted that this can lead to external influence on the authorities.

Is the authority to follow instructions by other public authorities/private parties?

There have not been registered any issues in that regard from responding countries.

Is there a possibility of judicial review to control the DSCs activities within the State?

All responding states indicated that there is a possibility of initiating proceedings, mainly before administrative courts.

If no: Why has your State not designated a DSC yet?

All EU-Member states which took part in this study have already designated a DSC.

Has your State set any other preparatory measures in order to designate a DSC by 17 February 2024? Please include all relevant information.

Germany has designated its DSC with the Digitale-Dienste-Gesetz (DDG).[16] Portugal has designated ANACOM as its DSC with Decree-Law n. º 20-B/2024[17] but has not yet tabled further legislation.

[16] Cf. (in German) https://gesetz-digitale-dienste.de

[17] Decreto-Lei n.º 20-B/2024 of 16 February 2024, Diário da República n.º 34/2024, 1º Suplemento, Série I, p.2.

How will the DSC have access to the data of intermediary services?

Competences of the DSC (Please consider the requirements of Article 51 DSA when answering the following questions):

Will the designated DSC have sufficient access to the data of intermediary services to perform its tasks? How is this access to data guaranteed under national law? What is the process of gaining access?

To enable DSCs to carry out their tasks, the DSA includes a list of powers that shall be given to DSCs. This includes the power of DSCs to request relevant information from providers and other persons related to the platform (see Article 51 (1a) DSA). The assignment of these powers to DSCs requires national legislation (Article 51 (6) DSA).

Only a limited number of replies have been provided for this question as several States have not yet adopted a law on this topic.

The report on Finland shows that a law has been adopted that gives the national authorities the power to obtain necessary data from providers or other persons (Article 51 (1a) DSA). To gain access to the information, the national authority has to request it. It has to be handed over without undue delay and free of charge (Section 4).

The Austrian KDD-G („Koordinator-für-digitale-Dienste-Gesetz) as well as the Italian legislation assign the power to request information of service providers and other persons (Article 51 (1a) DSA) to the national DSC.

The German law DDG includes a provision that mirrors the DSA's requirements. It also states that those obliged to provide information may deny access to data if it would expose them to the risk of criminal prosecution.

Will the designated DSC have sufficient access to the data of organizations performing the audits referred to in Article 37 and Article 75 (2) DSA to perform its tasks? How is this access to data guaranteed under national law? What is the process of gaining access?

Only a limited number of replies indicate such a provision, as many states have not implemented the necessary legislation yet.

Finnish and Austrian legislation allows the National DSCs to request the necessary information from persons performing the audit. The German legislation includes a similar provision.

Does the DSC have the power to accept the commitments offered by those providers in relation to their compliance with this Regulation and to make those commitments binding?

Only limited information is available. Both Finland and Austria allow DSCs to accept commitments and make them binding. The German law includes a similar provision.

Does the DSC have the power to order the cessation of infringements and, where appropriate, to impose remedies proportionate to the infringement and necessary to bring the infringement effectively to an end, or to request a national judicial authority to do so?

The Austrian DSC has been given this power; the German law includes a similar provision. The report on Finland refers to the national DSCs powers to impose fines. The report on Cyprus mentions that no such power has given to the DSC yet, but it is expected that corresponding legislation will be established soon.

Does the DSC have the power to impose fines, or to request a national judicial authority to do so?

The two reports on Austria and Finland show that legislation has been put in place that allows the DSC to impose fines. The German law includes a similar provision. Other reports show that most states have not yet implemented such legislation.

Does the DSC have the power to impose a periodic penalty payment, or to request a national judicial authority to do so?

Under Finnish, German and Austrian legislation: yes. There is no information available on other states.

Does the DSC have the power to adopt interim measures or to request the competent national judicial authority in their Member State to do so, to avoid the risk of serious harm?

Under the Austrian legislation, the DSC has been given this power, the German law includes a similar provision. Other reports do not indicate any national legislation on this topic.

What are the sanctions to be imposed by the Member States in case of infringements of the DSA by the intermediary services providers?

What are the penalties to be imposed by the Member States in case of infringements of the DSA by the providers of intermediary services?

Legislation in Finland, Austria, Germany, Italy, and Cyprus provides for sanctions in the form of monetary fees. There is no further information available on Cyprus. In Finland and Austria, the penalty depends on the form of infringement of DSA provisions. In both legislations, the amount which has to be paid mirrors the requirements of such penalties set out in Article 52 DSA.

Are these penalties effective, proportionate, and dissuasive?

As mentioned before, limited information on national legislation is available. Whether the penalties set out are effective cannot be examined at this time. However, Finland as well as Austria, Germany and Italy implemented detailed provisions on penalties, mentioning the different cases in which penalties are to be imposed and provisions on enforcement.

Do the penalties fulfill the requirements of Article 52 (3) DSA?[18]

As mentioned before, there is only limited information available. The Finnish, German, Italian, and Austrian legislation, which is already in force, fulfill the requirements of the DSA.

Do the penalties fulfill the requirements of Article 52 (4) DSA? (maximum amount of a periodic penalty payment: 5 % of the average daily worldwide turnover or income of the provider of intermediary services concerned in the preceding financial year per day, calculated from the date specified in the decision concerned)

As mentioned before, there is only limited information available. The Finnish, German, Italian, and Austrian legislation, which is already in force, fulfill the requirements of the DSA.

How is cooperation between national authorities structured? Are there any guidelines on cooperation with other national DSCs? If yes, how is such cooperation structured?

In some states, national legislation is in place that requires national authorities to cooperate within their own state. For example, in Finland, the national authority cooperates with the Data Protection Ombudsman and the Consumer Protection Ombudsman. In Austria, cooperation between the KommAustria (appointed DSC) and the public security services is established. In addition, KommAustria is required to regularly interact and exchange their opinions and experiences regarding certain topics with other DSCs. A similar provision is included in § 19 German law DDG. In Italy, the national DSC is authorised to sign cooperation agreements.

What obligations exist for companies not covered by the DSA?

On the EU-Level there are several legal acts besides the DSA which contain obligations for companies: GDPR, Terrorist Content Online Regulation[19], DSM Directive, Audiovisual Media Services Directive, Platform to Business (P2B) Regulation[20], DMA etc. The aim of the DMA is to make the digital markets sector fair and more contestable. The DMA applies to gatekeepers, which are defined as large digital platforms providing core platform services, designated pursuant to Article 3 (Article 2 (1) DMA). The DMA contains two lists with dos (Article 5 DMA) and do nots (Article 6) for companies acc. Article 3 DMA. In contrast to the DMA, the aim of the Terrorist Content Online Regulation is to combat and reduce

[18] Maximum amount of fines for a failure to comply with an obligation laid down in the DSA: 6 % of the annual worldwide turnover of the provider of intermediary services concerned in the preceeding financial year; maximum amount of fines for the supply of incorrect, incomplete or misleading information, failure to reply or rectify incorrect, incomplete or misleading information and failure to submit to an inspection: 1 % of the annual income or worldwide turnover of the provider of intermediary services or person concerned in the preceding financial year.

[19] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, OJEU 2021 L172/79.

[20] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, L186/57.

malicious content. Like Article 14 DSA, Article 5 (2) of the Terrorist Content Regulation contains the duty for intermediaries to take the fundamental rights of their users into account.

What are the rules regarding the evaluation of systemic risks (if complementary to those in the DSA)?

On 16 January 2023 the EU-Directive on the Resilience of Critical Entities (CER-Directive)[21] and the EU Directive on measures for a common level of cybersecurity across the Union (NIS2-Directive)[22] came into force. According to the CER Directive every member state shall create a national strategy to enhance the resilience of critical entities. The digital infrastructure which includes intermediary service providers is one of the eleven sectors which is covered by the Directive. According to the EU Directive EU member states must develop a national strategy and conduct regular risk assessments at least every four years. The aim of this risk assessment is to identify entities which are critical for society and economy. The EU member states must support entities which are considered critical. The NIS2-Directive also obliges EU-Member states to develop a national cybersecurity strategy which includes a risk management assessment system. Cypriot government has adopted the CER-Directive in its national legal framework and has created a specific agency on the topic of cybersecurity. The EU Directives must be implemented into national law by the end of 2024. In Germany, Austria, Cyprus and Finland the implementation is not done yet.

How is the integration of civil society structured?

According to Article 45 (2) DSA civil society must support the preparation of the code of conduct. The countries gave no information on the structure of the integration of civil society. The German DDG contains a section (§ 21 DDG) including civil society members in its *Beirat* (advisory board).

Is there an advisory board to raise the quality of the democratic feedback of the development of rules and practices of the platforms?

Among the surveyed countries Austria, Cyprus, Czechia, Finland and Portugal responded that they do not have such an advisory board. The German DDG contains a section including civil society members in its *Beirat* (advisory board).

[21] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, OJEU 2022, L 333/164.

[22] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJEU 2022 L333/80.

EU COST Action – CA19143: Global Digital Human Rights Network

The GDHRNet COST Action will systematically explore the theoretical and practical challenges posed by the online context to the protection of human rights. The network will address whether international human rights law is sufficiently detailed to enable governments and private online companies to understand their respective obligations vis-à-vis human rights protection online. It will evaluate how national governments have responded to the task of providing a regulatory framework for online companies and how these companies have transposed the obligation to protect human rights and combat hate speech online into their community standards. The matters of transparency and accountability will be explored, through the lens of corporate social responsibility.

The Action will propose a comprehensive system of human rights protection online, in the form of recommendations of the content assessment obligation by online companies, directed to the companies themselves, European and international policy organs, governments and the general public. The Action will also develop a model which minimises the risk of arbitrary assessment of online content and instead solidifies standards which are used during content assessment; and maximises the transparency of the outcome.

The Action will achieve scientific breakthroughs (a) by means of a quantitative and qualitative assessment of whether private Internet companies' provide comparable protection of human rights online in comparison with judicial institutions, and (b) in the form of a novel holistic theoretical approach to the potential role of artificial intelligence in protecting human rights online, and (c) by providing policy suggestions for private balancing of fundamental rights online.

Contact: Dr Mart SUSI, Action Chair, mart.susi@tlu.ee

Dr Vygante MILASIUTE, Action Vice Chair, vygante.milasiute@tf.vu.lt

Ms Laurena KALAJA, Science Communications Manager, laurenakalaja@hotmail.com