EBU
OPERATING EUROVISION AND EURORADIO

PUBLIC VERSION

DIGITAL SERVICES ACT

A HANDBOOK FOR PUBLIC SERVICE MEDIA

EBU LEGAL & POLICY

NOVEMBER 2024

CONTENTS

1. INTRODUCTION **3**

2. IN A NUTSHELL **4**

2.1. What is the DSA? 4

2.2. Why does the DSA matter to PSM? 4

2.3.1. What kind of digital services fall in the DSA's scope? 4

2.3.2. Which digital services will not be regulated by the DSA? 6

2.4. Who enforces and scrutinizes compliance with the DSA? 7

2.5. What is the relationship with other EU and national laws (in the field of media)? 7

2.6. When does the DSA enter into force? 7

3. LEGAL OBLIGATIONS RELEVANT FOR EBU MEMBERS AS BUSINESS USERS OF DIGITAL SERVICES **8**

3.1. Content moderation: Terms and conditions, their application and complaint procedures (Articles 14, 17, 20 and 21) **8**

3.2. Tackling illegal content: Notice & Action mechanism (Article 16) und the role of Trusted Flaggers (Article 22) 13

3.3. Systemic risks assessment and mitigation (Articles 34 and 35) 14

3.4. Crisis response mechanism (Article 36) and crisis protocols (Article 48) 15

3.5. Codes of Conduct (Articles 45, 46 and 47) 15

3.6. Transparency of recommender systems (Articles 27) and alternative options for recommender systems (Article 38) 16

3.7. Traceability of Traders (Article 30) 17

3.8. Right to lodge a complaint and seek compensation (Article 53 and 54) 17

4. CONCLUSIONS AND OUTLOOK **18**

1. INTRODUCTION

Welcome to this handbook on the Digital Services Act!

For some, law might be boring and hard to understand due to the jargon, cross-references, nitty-gritty definitions, and so on. Nevertheless, laws and regulations determine our lives, business operations, and almost every single part of society.

Big tech platforms have been unregulated for too long, although we may rather say "under-regulated". With the Digital Services Act (DSA) this will change. According to some leading politicians in Brussels, the DSA will bring order to the digital "Wild West". It is therefore important to understand what is in this EU law.

Aimed at making the Internet safer, more accountable and transparent, the DSA targets so-called "intermediary service providers" – which is the legal term used to describe all the digital services from social networks, to app stores and content-sharing platforms that are regulated by the Act. The DSA requires that these 'online platforms' take more responsibility regarding illegal information (goods, services, rental homes, texts, audio and audiovisual content, and more) offered on their services. The DSA also lays out important transparency requirements on the terms and conditions and recommender systems employed by these services to control access to and findability of content online. Furthermore, the DSA establishes certain rights for the users of such services, in particular when their content is removed of otherwise restricted.

Public service media (PSM) increasingly rely on third-party platforms to get their content and services to their audiences, in particular to the younger generation. Hence, the DSA also matters to EBU Members. With this handbook, the EBU aims to inform Members about the most relevant DSA provisions for PSM and how they may draw on them in their business operations and online activities.

This handbook is directed at PSM employees that work with third-party online platforms in the broadest sense, whether on the business, technical or legal side, and should provide answers to the most pressing questions they may have concerning the DSA.

2. IN A NUTSHELL

WHAT IS THE DSA?

The Digital Services Act (DSA) is an **EU law creating a single, uniform regulatory framework for intermediary services providers** that will be directly applicable across the EU. It lays out **rules and obligations concerning the design, operation, and processes** of such services with the aim to make the Internet safer, more transparent, predictable and accountable for the users of such services. The DSA does not impose any rules on the content which can be disseminated online, apart from the fact that what is illegal offline should also be illegal online and thus not be made available.

The DSA introduces **mechanisms to counter the availability of illegal content, goods and services** online, **safeguards for online users** whose content is removed or restricted by an online platform provider, and wide-ranging **transparency requirements**, including on terms and conditions and algorithmic recommendation systems. Even though the DSA is not a media legislation, it contains several provisions which will be useful for PSM in their relationships with third-party online platforms.

By the way: The DSA builds upon and updates the two-decades-old rulebook of the e-Commerce Directive. Adopted by EU institutions in 2000, the Directive established rather general rules for all kinds of online intermediation services and clarifications on their liability for content uploaded, stored and disseminated at the request of their users. The Directive prescribed, for instance, that no general obligation to monitor content should be imposed on online intermediaries.

Since 2000, the Internet has however changed considerably. New players have entered the market. In addition to internet access and cloud services, which play more or less exclusively the role of neutral services transmitting information, there are now social networks, search engines, app stores and many other providers that actively determine our digital lives. That is why, the EU saw the necessity to add a range of new, targeted obligations and mechanisms to the existing rulebook, in particular to improve the removal of illegal content and to protect users' fundamental rights online.

WHY DOES THE DSA MATTER TO PSM?

Beyond their own on-demand platforms and digital services, **PSM offer their content and services on a wide range of third-party online platforms** to reach and interact with their audiences, in particular young people. EBU Members offer their programmes for instance on social networks (Facebook, Instagram, Twitter and Snapchat) or content-sharing platforms (YouTube and TikTok).

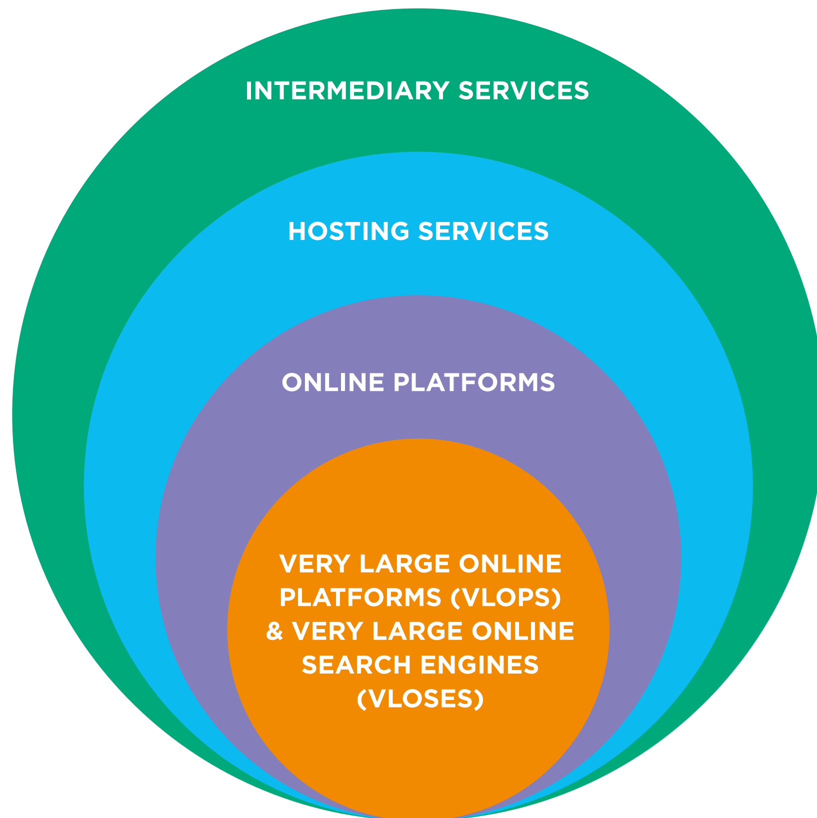
Yet, they also **depend on online platforms**, such as search engines (Google search) and app stores (Google Play, Apple App Store, Android App store), **through which many users find their digital offers**. This comes with certain challenges. Online platform providers unilaterally determine who sees what and when based on their algorithmic recommendation systems and terms and conditions.

As business users of online platform services, **PSM will benefit from certain obligations the DSA imposes on them**. Most importantly, PSM will be able to rely on additional procedural rights when they encounter issues with online platform providers. Hence, the DSA will add legal certainty and structure to the relationship between PSM and online platforms in certain areas.

WHAT KIND OF DIGITAL SERVICES FALL IN THE DSA'S SCOPE?

The DSA applies to a wide range of digital services – so-called **intermediary services** – that allow users to store and oftentimes share information, such as internet access services, cloud services, online marketplaces, rental platforms, **search engines, app stores, social networks or content-sharing platforms**. The DSA covers not only providers of intermediary services established in the EU, but also providers that are established outside the EU and that offer their services in the single market.

The DSA sets **asymmetric due diligence obligations** on different types of intermediaries **depending on the nature of their service as well as on their reach and societal impact**. The bigger and more socially significant a service is, the more stringent obligations it must fulfil. Consequently, the biggest players in the market – so-called very large online platforms (VLOPs) and very large online search engines (VLOSEs) – must comply with all of the rules, including the most far-reaching ones. By contrast, less consequential services only have to comply with some basic obligations.



- **Intermediary services** is the all-encompassing term for the services covered by the DSA. They include four different subcategories of services:
  (1) **mere conduit services** and (2) **caching services**, which offer network infrastructure services, such as Internet access services, domain name registrars, direct messaging services, virtual private networks, voice over IP;
  (3) **hosting services, including online platforms**; and (4) **online search engines**.
  All of these services must comply with the **universal obligations**, notably the creation of points of contact or legal representatives as well as requirements regarding the transparency, application and enforcement of their terms and conditions.

- **Hosting services** differ from the other subcategories of intermediary services in that they are not only a technical infrastructure but **allow users to store information** at their request. Relevant examples are **cloud services** (Drop Box, AWS) and **webhosting services**. These services must comply with **basic obligations**, such as allowing users to report illegal content.

- **Online platforms** are hosting services which **allow users to store and disseminate information at their request to the public** (unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service). Services, such as **social networks, app stores, content-sharing platforms or online marketplaces** fall in this category. They must respect **advanced obligations**, such as transparency requirements in terms of advertising and recommender systems, or complaint procedures. Micro- and small enterprises are however exempt from the rules applicable to online platforms. They must only fulfill the rules applicable to hosting services. In addition, even if micro- and small companies grow significantly, they remain exempt for a transitional period of 12 month.

- **Very large online platforms (VLOPs)** and **very large online search engines (VLOSEs)** are online platforms and search engines with an **average 45 million or more active users per month in the EU**. They are designated by the European Commission. The following services relevant for PSM will most likely fall in the category of VLOPs and VLOSEs: **Facebook, Instagram, TikTok, Twitter, YouTube, Google Play, Apple App Store, Google Search**. Considering their reach, these services pose particularly high risks to society and are therefore subject to the **most stringent requirements**.

	Intermediary Services	Hosting Services	Online Platforms	VLOPs	VLOSEs*
Requirements on terms and conditions (Article 14)	✔	✔	✔	✔	✔
Transparency reporting on content moderation (Article 15)	✔	✔	✔	✔	✔
Notice and Action mechanism / Removal of illegal content (Article 16)		✔	✔	✔	
Statement of reasons / Information to users on moderation decisions (Article 17)		✔	✔	✔	
Internal complaint-handling systems to challenge moderation decisions (Article 20)			✔	✔	
Out-of-court dispute settlement to challenge moderation decisions (Article 21)			✔	✔	
Trusted Flaggers (Article 22)			✔	✔	
Advertising Transparency (Article 26)			✔	✔	
Recommender Systems Transparency (Article 27)			✔	✔	
Obligation to keep an online advertising repository (Article 39)				✔	✔
Obligation to offer alternative recommender system (Article 38)				✔	✔
Risk assessment and mitigation (Articles 34 and 35)				✔	✔
Crisis response mechanism and crisis protocols (Article 36 and 48)			(✔)	✔	✔
Independent Audit (Article 37)				✔	✔
Data Access and Scrutiny (Article 40)				✔	✔

* Search engines are a special category of intermediary services. The asymmetric nature of the DSA does not fully apply. Very large online search engines (VLOSEs) must only comply with the universal obligations applicable to intermediary services in general, and with the most stringent obligations applicable to VLOPs.

WHO ENFORCES AND SCRUTINIZES COMPLIANCE WITH THE DSA?

The supervision and enforcement of the DSA rules will be shared between the European Commission and Member States.

The **European Commission** will be **solely responsible for overseeing and enforcing the most stringent obligations of the DSA** (Articles 33-43) **in relation to very large online platforms (VLOPs) and very large online search engines (VLOSEs)**. The supervision and enforcement of all other rules applicable to VLOPs and VLOSEs will be shared by the Commission and the Member States.

In addition, VLOPs and VLOSEs will undergo independent audits carried out by external organizations to assess compliance with the DSA. In case of a negative audit report, the platform operator must take the necessary measures to correct their misconduct. VLOPs and VLOSEs must also establish independent compliance officers, who will monitor compliance with the DSA internally. Upon request, VLOPs and VLOSEs will also have to grant the Commission and the Digital Services Coordinators (see below) access to data in order to monitor and assess compliance with the DSA.

Member States will **oversee all other intermediary service providers** that are established or have appointed a legal representative in their territory and that fall into the DSA's scope. They will be required to designate one competent national regulatory authority – the Digital Services Coordinator – for supervising compliance of the services with the new rules. Being a horizontal Regulation affecting many different sectors, the Digital Services Coordinator will cooperate with all other relevant national regulatory authorities (media, consumer protection, telecommunication, etc.) on the supervision and enforcement of the DSA.

For carrying out their tasks, the European Commission and the Digital Services Coordinators will, for example, be empowered to inspect the premises of a provider of intermediary services or to request other authorities to do so, in order to examine, seize, take or obtain information relating to a suspected infringement of the DSA. They will also have the power to impose fines of up to 6% of global revenue or remedies on a platform operator to cease any infringement.

WHAT IS THE RELATIONSHIP WITH OTHER EU AND NATIONAL LAWS (IN THE FIELD OF MEDIA)?

The DSA takes the form of an EU Regulation. Regulations are directly applicable and do not need to be transposed into national law. This means that any existing national law that conflicts with the DSA must be immediately set aside. The DSA leads to maximum harmonization, in the meaning that it prohibits Member States to impose additional rules at the national level on the matters falling within the scope of the DSA. Member States may of course still take measures in relation to intermediary services providers on issues falling outside the scope the DSA.

Being a "horizontal" instrument (that applies in all sectors), the DSA will coexist with and be complemented by sector-specific legislation (media, consumer protection, intellectual property, security, home affairs, etc.). Although the DSA states that it "is without prejudice to" sectorial laws at the EU level, the relationship between the DSA and the ability of Member States to take action in the interest of securing cultural diversity or media pluralism remains unclear and will ultimately need to be determined through its application, in particular, by the European Court of Justice.

WHEN DOES THE DSA ENTER INTO FORCE?

The DSA will enter into application in two steps. The DSA will be directly applicable to all intermediary services in February 2024. For VLOPs and VLOSEs, the new rules will kick in earlier: Once designated by the European Commission, they have four months to comply with the DSA (likely in spring/summer 2023).

3. LEGAL OBLIGATIONS RELEVANT FOR EBU MEMBERS AS BUSINESS USERS OF DIGITAL SERVICES

Content moderation: Terms and conditions, their application and complaint procedures (Articles 14, 17, 20 and 21)

DO INTERMEDIARY SERVICE PROVIDERS HAVE TO MODERATE CONTENT?

Yes and no. The DSA does not impose any general obligation on providers of intermediary services to moderate content that users posted on their services. But whenever content is flagged to them as being illegal, they do need to take action (see chapter on notice and action and trusted flaggers).

MAY INTERMEDIARY SERVICE PROVIDERS CONTINUE TO IMPOSE THEIR OWN CONTENT STANDARDS?

Yes. The DSA acknowledges the freedom of intermediary service providers to impose their own community standards and moderation policies on users in their **terms and conditions**. The DSA merely lays out **transparency requirements** and imposes **procedural obligations on the enforcement** of terms and conditions.

WHAT OBLIGATIONS DO INTERMEDIARY SERVICE PROVIDERS HAVE?

Intermediary service providers must **describe their content moderation practices**, including information on the reasons for imposing certain moderation decisions on content and the way these decisions are imposed, in their terms and conditions. They shall also explain whether, and if so how and when they use automation for content moderation. Providers must also **inform their users of any significant changes** they make to their terms and conditions. There is, however, no obligation to make this information available prior to imposing the changes.

Where an intermediary service is primarily directed at minors or is pre-dominantly used by them, the provider shall explain the conditions for and restrictions on the use of their service in a way that minors can understand. VLOPs and VLOSEs must publish their terms and conditions in the official languages of all Member States in which they offer their services.

Although, the DSA allows intermediary service providers to moderate content according to their own standards as defined in their terms and conditions, it does restrict their discretion in **how they apply and enforce their terms and conditions** to a certain degree. Notably, intermediary service providers must “pay due regard to the rights and legitimate interests of all parties involved, including […] freedom of expression, freedom and pluralism of the media». This amounts to a procedural requirement that intermediary service providers must assess the impact of their content-related decision-making on their users’ fundamental rights and try to limit arbitrary and erroneous content restrictions.

WHAT DOES IT MEAN FOR PSM?

PSM will be able to better understand the terms and conditions of intermediary service providers, as well as any changes made to them, due to the new transparency requirements.

PSM may encounter fewer arbitrary or erroneous content restrictions.

PSM will continue to encounter content removals and other kinds of interferences by intermediary service providers with their content and services. The DSA does not prohibit content moderation or the application of unilaterally imposed terms and conditions on editorial content and services.

WHAT HAPPENS WHEN A HOSTING SERVICE PROVIDER DECIDES TO MEDDLE WITH CONTENT?

In addition to making their terms and conditions transparent, hosting service providers, including online platform operators, must provide a clear and specific **statement of reasons when imposing restrictions on content** uploaded by their users. Users affected by a content moderation decision taken by such a provider must receive an explanation on the grounds and reasons behind the operator's decision.

A statement of reasons must be provided for any of the following restrictions imposed, at the latest at the moment the restriction is imposed:

(a) any restrictions of the visibility of a specific item of information, including removal of content, disabling access to content, or demoting content;
(b) suspension, termination or other restriction of monetary payments (monetization);
(c) suspension or termination of the provision of the service in whole or in part;
(d) suspension or termination of the recipient's accounts.

Hosting service providers must **explain the facts and circumstances relied on in taking the decision**, including whether the content is considered illegal or violating the platforms' terms and conditions. They must also refer to the concrete legal or contractual ground and explain why they consider the information to be illegal content or incompatible with their terms and conditions. Furthermore, hosting services must **inform the affected users about their possibilities to seek redress**.

WHAT DOES IT MEAN FOR PSM?

PSM will be informed whenever a hosting service provider takes down or restricts the visibility of their content or services. Situations, where PSM find out about content moderation decisions solely because they discover that audience numbers decline over a period time without any specific reason should not happen in the future anymore.

PSM will most likely be able to better understand why hosting service providers have taken any content moderation decision, thanks to the statements of reasons these providers will have to provide. This will improve PSM's ability to challenge the content moderation decisions of these providers.

PSM will only be informed once their content or services has already been interfered with by the hosting service providers. This is particularly problematic when the visibility of news content is restricted, which is most valuable for the audiences in the hours after publication.

Based on the statements of reasons, PSM can challenge content moderation decisions, either through the internal complaint-handling mechanisms, an out-of-court dispute settlement system or before a court in accordance with the applicable law. They will have to show that the decision was erroneous in the sense that the hosting service provider removed or restricted their content even though the content was neither illegal nor contrary to the terms and conditions. In certain cases, PSM may argue that the provider has not paid sufficient attention to the effects of its decision on the freedom and pluralism of the media, which is a requirement the DSA imposes on providers when they apply and enforce their terms and conditions.

The proposal for a European Media Freedom Act, published by the European Commission on 16 September 2022, contains specific obligations regarding content moderation by VLOPs in relation to media content and services. The Commission proposal foresees amongst other things that VLOPs must provide their statements of reasons to PSM and other media providers prior to imposing their decision. For the EBU, the Act offers an opportunity to advocate for stronger safeguards for PSM content and services on online platforms.

HOW CAN USERS COMPLAIN TO THE PROVIDER ABOUT AN UNJUSTIFIED DECISION?

In relation to online platform providers, the DSA establishes several procedures that users affected by content moderation can rely on to complain against and challenge decisions taken by a provider. Users can either directly complain to the platform provider using internal complaint-handling mechanisms, involve an out-of-court dispute settlement body or seek redress before national courts.

The DSA obliges online platform providers to establish **internal complaint-handling mechanisms**, enabling users to lodge a complaint, electronically and free of charge, against the action taken by the provider directly through the service. This possibility shall exist for a period of at least six months as of the day the user received the statement of reasons about the provider's decision.

The online platform providers must handle complaints submitted through their internal complaint-handling system "in a timely, nondiscriminatory, diligent and non-arbitrary manner" and "under the control of appropriately qualified staff, not solely on the basis of automated means". Where the affected user's complaint contains sufficient grounds for the platform provider to consider that its decision was not justified, the provider shall reverse its decision without undue delay. They must inform the user of their reasoned opinion and of the possibility of out-of-court dispute settlement and other available redress possibilities.

WHAT IF THE INTERNAL COMPLAINT-HANDLING MECHANISMS DOESN'T RESOLVE THE ISSUE?

In addition, users will be entitled to call on an **out-of-court dispute settlement body** to resolve disputes relating to content moderation decisions. Users may address these out-of-court dispute settlement bodies with complaints that could not be resolved by means of the internal complaint-handling mechanisms. Users may equally take their complaint directly to that body without going through the internal complaint-handling mechanism first. The competent out-of-court dispute settlement bodies will have to be certified by the Digital Services Coordinator of the Member State where the out-of-court dispute settlement body is established. In July 2024, the Maltese Digital Services Coordinator certified RGOAL Ltd., trading as "ADROIT" (Alternative Dispute Resolution Entity of Information Technology) as such a body, allowing EU-based users to review moderation decisions. Certification happens at the body's request, where it can demonstrate that it is impartial and independent, including financially, of any online platform provider and any platform user, and that it has the necessary expertise in relation to the issues arising from the availability of illegal content online, or in relation to the application and enforcement of terms and conditions.

Ultimately, users always have the right to bring their **complaint to a court** to contest content moderation decisions of any provider, even after invoking the internal complaint-handling mechanisms or the out-of-court dispute settlement system. They may initiate court proceedings at any stage in accordance with the applicable domestic law.

HOW LONG WILL THE DIFFERENT ROUTES TO CHALLENGE CONTENT MODERATION DECISIONS TAKE?

Likely too long, at least for media providers complaining about restrictions of time-sensitive content, such as news and current affairs programmes.

The DSA does not foresee any time limits for the **internal complain-handling mechanisms**. They only **need to be timely**. This provides online platform providers with some discretion in how quickly their mechanisms operate. The DSA does not allow for fast-track procedures or give priority to time-sensitive complaints of media services providers.

According to the DSA, **the certified out-of-court dispute settlement body** must make its solution available to the parties **within a reasonable period of time** and no later than 90 calendar days after the receipt of a complaint. In the case of highly complex disputes, the certified body may, at its own discretion, extend the 90 calendar days' time period to a maximum total duration of 180 days. The body's solutions are binding, although it does not have the power to impose them on the parties. In the case of non-compliance with the solution, the parties will have to turn to a court to order compliance or impose sanctions.

The duration of **court proceedings** will **depend on the national law**. Note that due to significant backlogs, court proceedings can take very long in some countries.

WHO PAYS FOR IT?

Although the **internal complaint-handling mechanisms** are most likely going to be free, users will have to pay any costs they accrue in order to bring a complaint themselves.

If the decision of the **out-of-court dispute settlement body** is in favour of the user, the online platform provider must bear the fees charged by the out-of-court dispute settlement body and reimburse the user for any other "reasonable expenses" that it has paid in relation to the dispute settlement. If the out-of-court dispute settlement body decides the dispute in favour of the online platform provider, the user must only reimburse any fees or other expenses that the online platform provider paid to the dispute settlement when the out-of-court dispute settlement body finds that the user manifestly acted in bad faith.

Finally, costs for **court proceedings** will be assigned according to national law. Often the losing party must bear the costs.

WHAT DOES IT MEAN FOR PSM?

PSM will be able to rely on different internal and external procedures to file complaints against content moderation decisions taken by online platform providers restricting access to their content and services. They will be able to make use of online platforms' own internal complaint-handling mechanism, out-of-court dispute settlement systems and court proceedings in no hierarchical order.

When using internal complaint-handling mechanisms, online platform providers will not be allowed to deal with PSM complaints solely by automated means, but must ensure that complaints are handled under the control of appropriately qualified staff. This will likely lead to better handling of PSM complaints by online platform providers in the future.

Online platform providers will retain some discretion regarding the timeframe for the handling of complaints. There is no fast-track procedure or priority for media organizations or other business users of online platform services. Hence, EBU Members' complaints will most likely be treated in the same way as those of ordinary users.

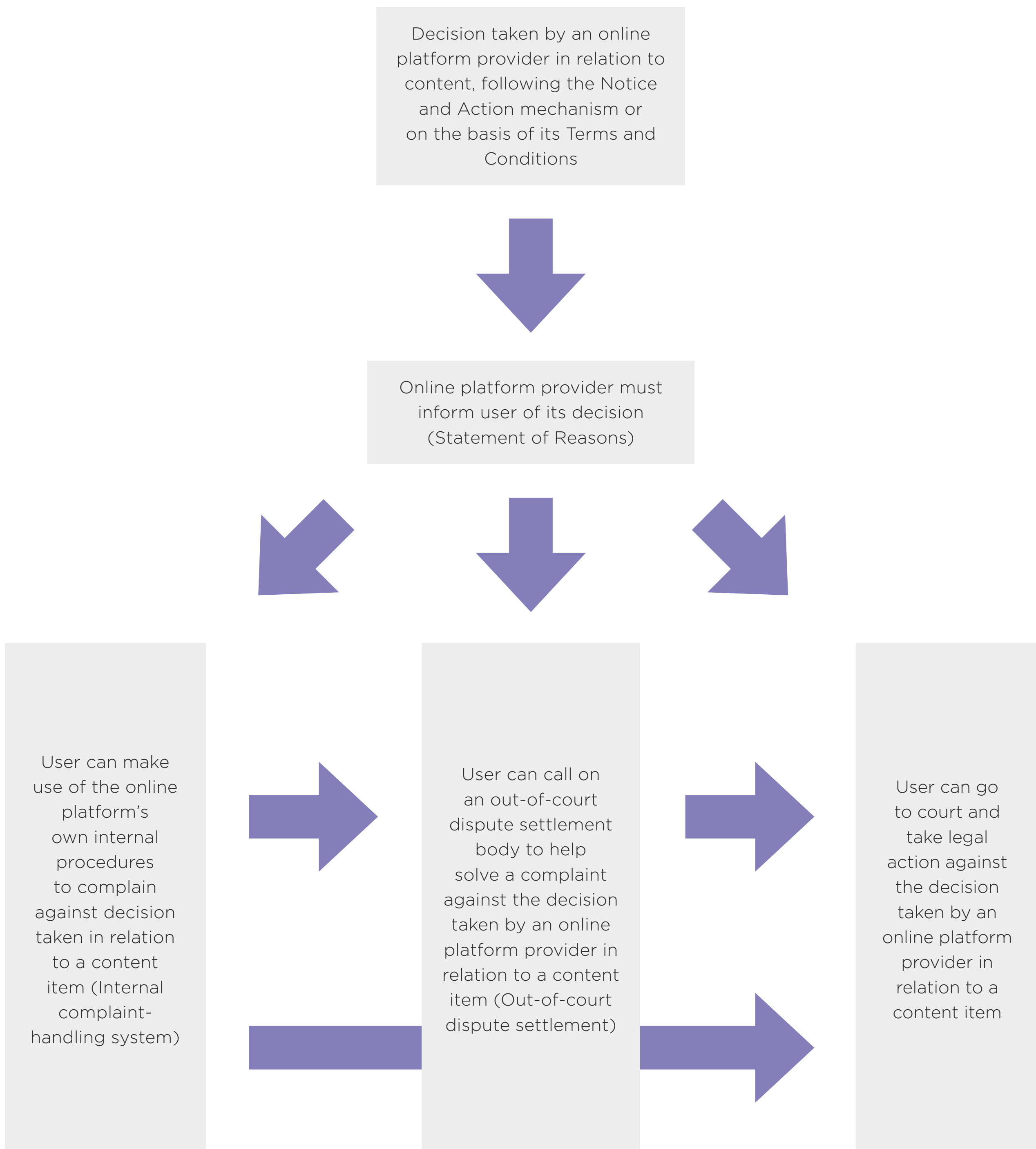
PSM will also be able to file their complaints with a neutral and competent out-of-court dispute settlement body. By going through such bodies, EBU Members' can avoid any potential biases of internal complaint-handling mechanisms.

The internal complaint-handling mechanism, the out-of-court dispute settlement systems and court proceedings will most likely take too much time and could be relatively cost-intensive. They are unlikely to provide an effective remedy against unjustified interferences with news content and other time-sensitive media content.

It might, however, be worth bringing a complaint in any of the above-mentioned fora in case the same or very similar issues repeat themselves. Even though it may not resolve the particular issue in time, it may create a precedence that will speed up the process for similar incidents in the future.

The proposal for a European Media Freedom Act, published by the European Commission on 16 September 2022, contains specific obligations regarding content moderation by VLOPs in relation to editorial content and services. The Act foresees amongst other things that VLOPs must treat complaints by media providers, including PSM, with priority and without undue delay. For the EBU, this legislative initiative offers an opportunity to advocate for further finetuning the relationship between online platforms and PSM.

OVERVIEW OF THE DIFFERENT ROUTES TO CHALLENGE ONLINE PLATFORM PROVIDERS' CONTENT MODERATION DECISIONS UNDER THE DSA:



Tackling illegal content: Notice & Action mechanism (Article 16) und the role of Trusted Flaggers (Article 22)

WHAT OBLIGATIONS DO HOSTING SERVICES AND ONLINE PLATFORMS HAVE TO REMOVE ILLEGAL CONTENT?

The DSA does not impose a general obligation on hosting service providers, including online platforms, to detect and remove illegal content from their services. Instead, it obliges them to put in place **Notice and Action mechanisms enabling users to notify them of the presence on their service of specific items of information that the users consider to be illegal**. They must make sure that these mechanisms are easy to access, user-friendly, and allow for the submission of notices exclusively by electronic means. Notices must contain all of the following elements:

- a sufficiently substantiated explanation of the reasons why the individual or entity alleges the information in question to be illegal content;
- a clear indication of the exact electronic location of that information, such as the exact URL or URLs, and, where necessary, additional information enabling the identification of the illegal content adapted to the type of content and to the specific type of hosting service;
- the name and an electronic mail address of the user submitting the notice;
- a statement confirming the good faith belief of the user submitting the notice that the information and allegations contained therein are accurate and complete.

Once hosting service providers have received a notice on an alleged illegal information on their service, they must process it "in a timely, diligent, non-arbitrary and objective manner" and inform the user of their decision in respect of the information without undue delay, providing also information on the redress possibilities the user can invoke in case they are not satisfied by the provider's handling of the notice. Where hosting service providers consider notified content to be illegal, they must remove it from their service or block access to it.

WHAT COUNTS AS ILLEGAL CONTENT UNDER THE DSA?

The DSA itself does not harmonize what information, content or behavior counts as illegal. Instead, it refers to the whole EU legal acquis, including national laws, which define what is illegal (e.g., copyright infringements, hate speech, selling of certain products, child sexual abuse material, terrorist content).

WHAT IS A TRUSTED FLAGGER AND WHO CAN BECOME ONE?

Certain entities, but not individual users, can apply to become so-called "**trusted flaggers**". Notices flagging illegal content submitted by trusted flaggers must be treated preferentially: Online platform providers must process and decide upon these notices with priority and without undue delay.

The Trusted Flaggers status can be awarded to any entity which fulfills the following conditions:

- it has particular expertise and competence for the purposes of detecting, identifying and notifying illegal content;
- it is independent from any provider of online platforms;
- it carries out its activities for the purposes of submitting notices in a diligent, accurate and objective manner.

Interested entities must apply for the status with the Digital Services Coordinator of the Member State in which they are established.

The DSA further underlines that the overall number of trusted flaggers should be limited to avoid undermining this mechanism. If too many trusted flaggers submit notices flagging allegedly illegal content, online platform providers would arguably not be able to effectively grant priority to their notices anymore. Therefore, the DSA suggests that in particular industry associations representing their members' interests should apply for the status of trusted flaggers. At the same time, the DSA does not prevent private entities or individuals from entering into bilateral agreements with online platform providers over the possibility to flag potentially illegal content on a preferential basis, as is already the case today.

WHAT OBLIGATIONS DO TRUSTED FLAGGERS HAVE?

The trusted flaggers status comes not only with certain rights, but also with obligations. Trusted flaggers must publish, at least once a year, easily comprehensible and detailed reports on the notices they submitted. The report must list, at least, the number of notices submitted categorized by (a) the identity of the online platform provider, (b) the type of allegedly illegal content notified, and (c) the action taken by the online platform provider.

The status of trusted flaggers can be revoked or suspended by the Digital Services Coordinator if it has reasonable doubts or determines that the entity no longer meets the above-mentioned conditions, either following an investigation on its own initiative, or on the basis of information received from third parties, including by the online platform provider. This can be the case when the trusted flagger submits a significant number of insufficiently precise, inaccurate, or inadequately substantiated notices.

WHAT DOES IT MEAN FOR PSM?

The Notice and Action mechanism could lead to situations where users flag PSM content as illegal, for instance for an alleged copyright infringement, and hosting service providers take it down erroneously.

For PSM, it could be useful to apply for the status of trusted flaggers as it would allow for a swift reaction by online platform providers when copyright infringements happen. It is, however, unclear whether individual EBU Members or the EBU would qualify to become trusted flaggers under the DSA. Furthermore, it is unclear whether the costs do not outweigh the benefits of being a trusted flagger, as the status also comes with reporting obligations.

Systemic risks assessment and mitigation (Articles 34 and 35)

WHAT ARE SYSTEMIC RISKS AND HOW DOES THE DSA TACKLE THEM?

The DSA introduces specific obligations for very large online platforms (VLOPs) and very large online search engines (VLOSEs) to identify, analyze and assess any **systemic risks stemming from the design, including algorithmic systems, functioning and use made of their services** and take measures to mitigate them. They shall carry out such exercise at least once every year and pay particular regard to the following risk areas:

- the **dissemination of illegal content** through their services (e.g., hate speech, copyright infringements or counterfeits, bullying, stalking, child abuse material, unsafe products, etc.);
- any actual or foreseeable **negative effects of their service for the exercise of fundamental rights** (e.g., freedom of expression and information, including freedom and pluralism of the media pluralism);
- any actual or foreseeable **negative effects on civic discourse, electoral processes, and public security**;
- any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health, minors and serious negative consequences to the person's physical and mental well-being.

VLOPs and VLOSEs must preserve all supporting documents of their risk assessments for at least three years after the performance of risk assessment, and shall, upon request, share them with the Commission and the Digital Services Coordinator of establishment.

WHAT MUST PLATFORMS DO TO MITIGATE SYSTEMIC RISKS?

To mitigate the systemic risks, the typical actions expected to be taken by VLOPs and VLOSEs include

- adapting their recommender systems and algorithmic systems;
- adjusting their terms and conditions and their enforcement;
- introducing specific protection measures in favor of vulnerable groups;
- marking of deep fakes;
- adapting their content moderation processes for illegal content, including the speed and quality of processing notices and the expeditious removal of or disabling access to certain kinds of illegal content, for example illegal hate speech or cyber violence;
- adjusting cooperation with trusted flaggers;
- implementing decisions of out-of-court dispute settlement bodies.

When taking any measures to mitigate systemic risks, VLOPS and VLOSEs shall pay particular consideration to the impacts of such measures on fundamental rights.

HOW WILL THE EU ASSIST PLATFORMS IN MITIGATING SYSTEMIC RISKS?

The European Commission, in cooperation with the Digital Services Coordinators, can issue guidelines with the aim of presenting best practice examples and recommend possible risk mitigation measures. When preparing those guidelines, the European Commission shall organize public consultations.

Once a year, the European Board for Digital Services, in cooperation with the Commission, shall publish comprehensive reports on the most prominent and recurrent systemic risks reported by VLOPs and VLOSEs or identified through other information sources as well as best practices to mitigate these risks.

WHAT DOES IT MEAN FOR PSM?

The risk assessment and mitigation exercise might open the door for the EBU and Members to address directly with VLOPs and VLOSEs some of the challenges PSM face. For instance, it could be an opportunity to work together with these platforms on specific measures to ensure that reliable information by trusted media is available, for instance to counter disinformation. There is, however, no legal obligation for these platforms to consult business users, such as PSM, on possible systemic risks and their mitigation.

Crisis response mechanism (Article 36) and crisis protocols (Article 48)

WHAT MUST PLATFORMS DO IN THE FACE OF A CRISIS?

In times of crisis, i.e., a pandemic, a natural disaster or an armed conflict, the DSA's crisis response mechanism empowers the European Commission, acting upon a recommendation of the European Board for Digital Services, to require very large online platforms (VLOPs) and very large online search engines (VLOSEs) to make **specific risk assessments** and take specific risk mitigation measures tailored to the relevant crisis.

VLOPs and VLOSEs will need to assess whether and how the functioning and use of their services contribute to the crisis. Moreover, they will need to identify and apply specific, effective and proportionate measures to prevent, eliminate or limit any such contribution to the risks identified. They must report to the Commission on the risks identified and the measures taken.

WILL PLATFORMS HAVE TO PREPARE FOR POSSIBLE CRISIS SITUATIONS?

To ensure effective action on the part of VLOPs and VLOSEs during a possible crisis, the European Board for Digital Services may also recommend the Commission to initiate the drawing up of **voluntary crisis protocols** for addressing possible crisis situations affecting public security or public health. VLOPs, VLOSEs and, where appropriate, other online platform providers should participate in this exercise. The European Commission can also involve Member States' authorities, Union bodies, civil society organizations and other relevant stakeholders in drawing up the crisis protocols.

The DSA describes that one or more of the following measures should be part of such voluntary crisis protocols:

- prominent displaying of information on the crisis situation provided by Member States' authorities or at Union level or by other relevant reliable bodies;
- ensuring that the online platform provider appoints a specific point of contact responsible for crisis management;
- where applicable, adaptation of the resources dedicated to the tackling of illegal content, content moderation or the mitigation of systemic risks to the needs created by the crisis situation.

Every crisis protocol must set out clearly what kind of crisis they aim to address, how the crisis protocol is to be activated and for how long the measures identified to mitigate the crisis should be implemented.

WHAT DOES IT MEAN FOR PSM?

Equally to the systemic risk assessment and mitigation exercise, PSM could get involved in the drawing up of the voluntary crisis protocols and push for specific mitigation measures VLOPs and VLOSEs should take during a crisis.

Codes of Conduct (Articles 45, 46 and 47)

WHAT IS THE ROLE OF CODES OF CONDUCT UNDER THE DSA?

To give further substance to the many due diligence obligations laid down in the DSA, the European Commission and the European Board for Digital Services will encourage and facilitate the development of so-called Codes of Conduct. Although Codes of Conduct are not binding, they may be very persuasive because they **codify what kinds of conduct are not only permissible but even desirable** under a certain law. In the context of the DSA, they may **assist online platforms in ensuring compliance with various otherwise vague due diligence obgligations**. Indeed, the existence of these Codes of Conduct will make it difficult for platform providers to deviate from the standard practices they codify.

By the way: A Code of Conduct is a co-regulatory instrument, developed in cooperation between the European Commission and intermediary service providers. Also, relevant competent authorities, civil society organizations and other stakeholders can be invited to participate in the drawing up these Codes. They usually set out commitments for their signatories to take specific measures to achieve certain objectives. Becoming a signatory of a Code of Conduct is completely voluntary.

WHAT CODES OF CONDUCT DOES THE DSA ENVISAGE?

The DSA explicitly envisages the drawing up of two Codes. One should further **transparency in the online advertising value chain** beyond the transparency requirements already set out in the DSA. Another one should promote **full and effective equal participation of persons with disabilities** by improving the accessibility to online services. The existing **Code of Practice on Disinformation**[2] will also become a Code of Conduct recognized under the DSA.

WHAT DOES IT MEAN FOR PSM?

PSM could contribute to the drawing up of any relevant Code of Conduct. Considering the increasing shift of advertising revenues from the media to online platforms, it might be interesting for EBU Members to be involved in the drafting of the future Code of Conduct on transparency in the online advertising value chain.

PSM could advocate for media-specific Codes of Conduct to support the proper application of the DSA, in particular with regards to the risks for media freedom and pluralism stemming from the design, functioning and use made of VLOPs' and VLOSEs' services.

2. The existing Code of Practice on Disinformation has been signed on 16 June 2022. It builds on the previous Code from 2018. 34 organisations and businesses have committed to the Code so far. For signatories that are very large online platforms or very large search engines, committing to the Code is considered as complying with the obligation to mitigate certain systemic risks (disinformation) under the DSA.

Transparency of recommender systems (Article 27) and alternative options for recommender systems (Article 38)

WILL PLATFORMS HAVE TO DISCLOSE THEIR ALGORITHMIC RECOMMENDER SYSTEMS?

No, the DSA does not oblige platforms to fully disclose their algorithmic recommender systems. However, all online platforms will have to clearly **explain in their terms and conditions the main parameters** they use to recommend information to their users (e.g., timelines, suggestion tools, recommended video sections, etc.), as well as any options for users to modify or influence those parameters.

WILL USERS BE ABLE TO OPT OUT OF THE PLATFORMS' RECOMMENDER SYSTEMS?

It is not obligatory for online platforms to offer different options of recommender systems to their users. But where they do offer alternative recommender systems, users must be enabled to select and to modify their preferred option at any time. By contrast, VLOPs must always offer at least one alternative option that is not based on the profiling of their users for each of their recommender systems. However, this option does not have to be the default option.

WHAT DOES IT MEAN FOR PSM?

The recommender systems used by online platform providers to rank, prioritize, and suggest content, including the content of PSM, have so far been a black box. In the future, online platforms must increase the transparency of their recommender systems. This might help PSM better understand why certain content is (not) seen by users.

EBU and Members could promote the use of 'public-value' algorithms or criteria, promoting amongst other things PSM content and services, given that VLOPs will have to offer at least one alternative recommender system which is not based on user profiling.

Traceability of Traders (Article 30)

HOW DO ONLINE PLATFORMS HAVE TO ENSURE THE TRACEABILITY OF TRADERS?

The DSA requires certain online platforms, namely those that allow users to enter into distance contracts with traders, such as online marketplaces or app stores, to ensure that their platforms are a safe place to buy goods or services. It requires online platform providers to collect certain information about traders offering goods or services on their platforms, such as their name, telephone number and email address, and trade registration number where applicable. Online platforms must then use their best endeavours to verify this information against publicly available records or databases. The 'know your business customer' requirement thus helps to prevent fraudulent activity on such platforms and discourages traders from offering illegal products or services to consumers.

WHAT DOES IT MEAN FOR PSM?

PSM may be considered as traders under the DSA. The term 'trader' is broadly defined as "any natural person, or any legal person irrespective of whether it is privately or publicly owned, who is acting [...] for purposes relating to his or her trade, business, craft or profession". The traceability requirement incumbent on platform providers may therefore have an impact on PSMs when they offer services/ content on those platforms that allow for the conclusion of distance contracts. For the definition of «distance contract», the DSA refers to the Consumer Rights Directive, which covers not only contracts where the consumer pays a price, but also contracts or agreements relating to a digital service where the consumer provides personal data to the trader. This is the case, for example, when PSMs make applications available on app stores.

Right to lodge a complaint and seek compensation (Article 53 and 54)

WHAT CAN USERS DO WHEN AN ONLINE SERVICE BREACHES THE DSA?

Users, both individuals and entities, have the right to lodge a complaint against intermediary service providers for violating the DSA rules and obligations with the Digital Services Coordinator of the Member States where the user is located or established. If they are (financially) affected by breaches of the DSA's obligations, they can also seek compensation from the intermediary service provider before national courts. Such claims are often specified in national law, such as competition law, consumer law, intellectual property law, or general tort law.

WHAT DOES IT MEAN FOR PSM?

PSM could lodge complaints or seek compensation in case intermediary service providers infringe the rules of the DSA. For example, if a hosting service removes or reduces the visibility of a content item without providing a statement of reasons informing about and explaining its decision, the media organization would have the right to complain about the provider's behavior to the national Digital Services Coordinator or the European Commission.

4. CONCLUSIONS AND OUTLOOK

Public service media will benefit, to a certain extent, from the DSA and the obligations it imposes on intermediary service providers. The DSA will add structure to the relationship between EBU Members and the third-party online platforms they operate on, such as Facebook, Instagram, Snapchat and TikTok, and increase accountability and transparency of the ways these platforms function, design their services, and take decisions.

However, the DSA will not resolve all the problems EBU Members encounter in the digital realm. In all likelihood, they will continue to be confronted with online platform providers removing or meddling with their content and services. The DSA provides for few restrictions on the design, application and enforcement of terms and conditions. The recourse possibilities the DSA establishes whenever an online platform removes PSM content or restricts its visibility will also not be adequate for EBU Members' needs in most cases. The DSA also fails to fully unlock the black box of recommender systems.

In consequence, PSM as well as all other media providers offering their content and services online will depend on sector-specific laws, which acknowledge and address the specific needs of and challenges media face vis-à-vis third-party online platforms.

The recently proposed European Media Freedom Act might thus provide an opportunity for the EBU and its Members to correct (some of) the shortcomings of the DSA and add media-specific regulatory solutions to the horizontal rules of the DSA. The proposed Regulation contains, for instance, a provision equipping media service providers with additional rights in the face of arbitrary content removals. The EBU Legal & Policy community will work towards further strengthening media providers' rights vis-à-vis platform operators throughout the legislative process.

However, regulatory solutions alone, whether through the DSA or the upcoming European Media Freedom Act, will most likely not solve all the problems EBU Members face in relation to third-party online platforms. The EBU and its Members should therefore continue to build the best possible (operational) relationships with online platform providers. Good contacts are necessary so that PSM can raise and possibly resolve conflicts as quickly as possible. Informal discussion channels between PSM and the platforms they operate on can just as well help to jointly work out practical solutions to various problematic issues. For online platform providers, it could even be beneficial to collaborate with PSM to comply with some of the new obligations created by the DSA.

In that sense, it will be important that the different departments within the EBU and the membership work together to ensure that PSM can thrive and operate in the online environment without far-reaching restrictions imposed unilaterally by the platforms acting as intermediaries between us and our audiences.

ABOUT THE EBU LEGAL & POLICY DEPARTMENT

In a fast-changing technological, political and regulatory environment, we advise our Members on specific regulatory issues, offering practical solutions in the fields of EU and national competition, copyright and media law that are specific to their needs.

We analyse legislative proposals, explore the implications with legislators and promote a legal framework which allows our Members to operate with optimum efficiency whilst continuing to contribute to the democratic, social and cultural needs of society.

We also manage EBU membership and statutory matters and advise on all EBU contracts, including the Eurovision Song Contest, sports, news and networks.

Sophia WISTEHUBE
Legal Counsel
wistehube@ebu.ch
T +41 22 717 2248

Thomas BERGMANN
Senior EU Policy Advisor
bergmann@ebu.ch
T +32 2 286 9103

Jenny WEINAND
Head of Media Law
weinand@ebu.ch
T +41 79 957 2779

ABOUT THE EBU

The European Broadcasting Union (EBU) is the world's leading alliance of public service media (PSM). We have 112 member organizations in 56 countries and have an additional 31 Associates in Asia, Africa, Australasia and the Americas. Our Members operate nearly 2,000 television, radio and online channels and services, and offer a wealth of content across other platforms. Together they reach an audience of more than one billion people around the world, broadcasting in 153 languages. We operate Eurovision and Euroradio services.

EUROPEAN BROADCASTING UNION

L'Ancienne-Route 17A
1218 Le Grand-Saconnex
Geneva, Switzerland
T +41 22 717 21 11
ebu@ebu.ch

Learn more about the EBU at
www.ebu.ch

Follow us on social media:

twitter.com/EBU_Policy

facebook.com/EBU.HQ

linkedin.com/company/EBU

instagram.com/ebu_hq