

Digital Services Act and

European Media Freedom Act

What they mean for content
moderation and media freedom

Contents

Introduction	3
Who is covered by the DSA and EMFA?	4
What protections do the DSA and EMFA provide against unfair content moderation?	6
Do the DSA or EMFA create any specific protections for media?	9
Do the DSA or EMFA create any new transparency obligations to help identify when moderation was unfair?	9
What counts as illegal content under the DSA and EMFA?	10
What responsibilities do digital platforms have to protect users from illegal content ?	10
What information must a digital platform provide on how they promote or target users with content (i.e. algorithm transparency)?	11
What do VLOPs and VLOSEs need to include in their risk assessments?	11
Is there a process for stakeholders to work with regulators on the content of risk assessments?	12
What powers do regulators have to require platforms to take specific actions after a risk assessment?	13
What rights do media organisations have to bring complaints to regulators and/or submit evidence?	14
DSA & EMFA Risk Checklist for Media	15
1. Confirm MSP Status & Eligibility	15
2. Manage Content Moderation Risk	16
3. Use Redress & Complaints Rights	16
4. Engage With VLOPs Proactively	16

Introduction

This Guide provides an overview of the implications of the [Digital Services Act \(DSA\)](#) and the [European Media Freedom Act \(EMFA\)](#) for journalists and other media service providers (MSPs) working with online service providers such as social media sites and search engines in the EU. The DSA focuses on creating a safer and more transparent online space by regulating digital services – particularly online platforms, hosting services, and very large online platforms (VLOPs) – across the EU. The EMFA, on the other hand, aims to strengthen media freedom, independence, and pluralism in the EU.

This Guide focuses on the responsibilities of online platforms when they moderate content, and the types of redress available to journalists who may be affected by those moderation decisions. Other parts of the EMFA relate to how MSPs interact with governments and national security actors, amongst other things. These elements are beyond the scope of this Guide.



Who is covered by the DSA and EMFA?

The DSA entered into force on 17 February 2024, but the Commission was allowed to designate platforms as VLOPs or “very large online search engines” (**VLOSEs**) earlier. If it did, the DSA applied to those entities four months after designation, even if that was before 17 February 2024.

The EMFA entered into force on 8 August 2025. It applies to all MSPs that target audiences in the EU, whether they are based inside or outside the EU.

The DSA is the EU’s main set of rules for how online content is handled. It sets out responsibilities for companies that store and share content produced by users – like social media platforms or online marketplaces. The DSA’s goal is to make sure the internet is a safer, more reliable, and more predictable place for everyone.

The DSA applies to “intermediary services”, which is an online service that helps move or store content – like passing messages between users, temporarily saving information to make websites load faster, or hosting content that people upload e.g.. There are then three defined entity types under this umbrella term:

Intermediary services under the DSA

1. **Hosting services** – A type of intermediary service that stores content – like texts, images, videos – that users upload or share, e.g. cloud and web hosting services
2. **Online platforms** – A type of hosting service that lets users upload content – like posts, videos, or listings – and then makes the content available to others on the internet, e.g. online marketplaces, app stores, platforms that connect individuals to rent or exchange things (e.g. homes, cars, or skills), and social media platforms
3. **VLOPs** – Online Platforms with over 45 million users in the EU – like social media or video sharing sites – and officially designated by the European Commission because of their size and influence

The DSA sets out rules for intermediary services, hosting services, online platforms, and VLOPs (as well as other actors not covered by this Guide). Any service that falls under the DSA must follow the specific rules for its category, as well as the rules for any broader group to which it belongs.

The EMFA, on the other hand, covers a broad range of MSPs – namely, entities that provide media services, e.g. television, radio broadcasts, podcasts and press publications, and who have editorial responsibility for their content.¹ The EMFA also applies to VLOPs. VLOPs can qualify as MSPs themselves,

¹ European Media Freedom Act – Article 2(2)

but more generally VLOPs act as gateways to content posted by users, which may include MSPs. The EMFA, therefore, imposes certain rules on VLOPs if and when they address content posted by MSPs.

The EMFA does not cover content created by users for personal or non-commercial purposes – such as private messages, comments or personal content. The EMFA has been criticised for using this traditional and service-based definition of media, which excludes amateur citizen journalists and NGOs. This is because the definition of ‘media service provider’² requires the relevant activities to be ‘normally ... provided for remuneration’³. As such, people or organisations who produce journalistic content with no intention of being remunerated do not seem to be covered.⁴

Covered entities under the EMFA

All types of media services, including television, radio, press and audio podcasts, public service broadcasters.

VLOPs – but only when they provide media services

Under the EMFA, VLOPs are required to include a feature that lets MSPs share certain information about themselves. In Article 18(1), the EMFA states that VLOPs must allow MSPs to state:

- that they are MSPs;
- that they comply with the obligation to provide certain information to their users, e.g. their legal name and general contact details, names of direct and indirect owners, names of beneficial owners, amounts of public funds received for state advertising, and advertising revenues from third-country public authorities or entities⁵;
- contact details through which the VLOP can communicate with them directly and quickly;
- that they are editorially independent from EU Member States, political parties, non-EU countries and entities controlled or financed by non-EU countries;
- that they follow editorial rules set by law in at least one EU country and are overseen by an official regulator. If not, they should show that they follow widely accepted industry standards through a recognised self-regulatory or co-regulatory body in the media sector;

2 European Media Freedom Act – Article 2

3 This is tied to the definition of ‘services’ under Art. 57 of the Treaty on the Functioning of the European Union (TFEU)

4 Horton, G. and Assersen-Skadberg, A. (2026) ‘European Media Freedom Act: can it stop the democratic backsliding?’, *Journal of Media Law*, pp. 1–23. doi: 10.1080/17577632.2025.2607101 and Seipp, T., Fathaigh, R. Ó., and van Drunen, M. (2023). ‘Defining the ‘media’ in Europe: pitfalls of the proposed European Media Freedom Act’, *Journal of Media Law*, pp. 39–51. doi: 10.1080/17577632.2023.2240998

5 European Media Freedom Act – Article 6(1)

- the contact details of the relevant national regulatory authorities or recognised industry bodies that oversee their editorial standards; and
- that they do not provide content generated by artificial intelligence systems without subjecting it to human review or editorial control.

The rules in the EMFA for how VLOPs handle content from MSPs only apply if the MSP has officially shared this information with the platform.

What protections do the DSA and EMFA provide against unfair content moderation?

The DSA and the EMFA set out rules to ensure any moderation⁶ of content carried out by hosting services, online platforms and VLOPs is handled fairly and transparently. These rules aim to protect the rights of media providers and the public's access to reliable information by providing clarity on rules before moderation, clarity on the specific reasons for any moderation decisions, and a right to challenge decisions.

Under the DSA and EMFA, online platforms must provide:

1. Information on content moderation activities in their terms and conditions

Under the DSA, intermediary services – including hosting services, online platforms, and VLOPs – must clearly explain in their terms and conditions any rules or limits they place on the content that users can share on their platforms.⁷ This includes automated algorithmic decision-making and human review. They must also share how their internal complaint system works, so that users understand how to raise concerns or challenge decisions.

2. Clear reasons when content restrictions are applied

Both the DSA and the EMFA require all entities that fall under their scope to provide users with clear and specific reasons when their content is restricted, removed, or downgraded.

Under Article 17 of the DSA, a hosting service (e.g. a social media platform or an online marketplace) must explain why it has decided to remove or restrict content posted by a user – i.e. because it is either illegal or breaks the platform's rules. This includes actions like:

⁶ The DSA defines “content moderation” as “the activities, whether automated or not, undertaken by providers of intermediary services that are aimed, in particular, at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, demonetisation, disabling of access to, or removal thereof, or that affect the ability of the recipients of the service to provide that information, such as the termination or suspension of a recipient’s account” (Art. 3(t)).

⁷ Digital Services Act – Article 14(1)

- taking down a post or limiting its visibility;
- stopping or restricting payments;
- stopping or suspending a service in whole or in part; or
- suspending or terminating the user's account.

When providing reasons to affected users, a hosting service provider must include the following information:

- what action it has taken – for example, whether the content was removed, made harder to find, had its visibility reduced, if any payments linked to the content were stopped, or if any other steps were taken (e.g. stopping payments, stopping or suspending a service). They also need to say how long the action will last, and where it applies;
- the reasons behind the provider's decision, including whether it was made because of a report they received or from their own investigation and, if strictly needed, who made the report;
- if automated tools were used to make the decision, whether the content was found or flagged by those tools;
- if the decision is about content that is claimed to be illegal, which law it is based on and why the content is considered illegal;
- if the decision is because the content does not follow the platform's rules, which rule was broken and why the content goes against it; and
- clear and easy-to-understand information about how users can challenge the decision. This includes options like filing a complaint with the platform, using outside dispute resolution services, or going to court.

Under Article 18 of the EMFA, VLOPs must take the following steps before deciding to suspend or limit the visibility of content from an MSP for breaking the platform's rules:

- It must provide the MSP with a statement of reasons that complies with the above requirements of the DSA, on a "durable medium"⁸ (i.e. something which the VLOP cannot edit after they've sent it to the MSP, such as a physical sheet of paper or an email, as opposed to a link to a webpage which the VLOP still controls); and
- Except in a crisis situation, it must give the MSP 24 hours to respond before taking any action to remove or restrict the content. If the VLOP still decides to go ahead with the removal or restriction of content, either after receiving a reply or if no reply is given, it must inform the media organisation without unnecessary delay.

The obligations do not apply, however, where the VLOP is complying with its obligations relating to illegal content or certain of their obligations under the DSA or [EU Directive 2010/13 \(the Audiovisual Media Services Directive or “AVMSD”\)](#).

3. Internal complaint-handling system and out-of-court dispute resolution.

Under Articles 20 and 21 of the DSA, online platforms, including VLOPs, must provide users with an effective internal complaint-handling system so that they can lodge complaints, electronically and free of charge. Users are given at least six months to lodge a complaint, starting from the day the user receives the notice or from the day the decision is taken by the provider on the grounds that the content is illegal or goes against the provider’s terms and conditions. These decisions may be on whether to:

- 
- remove or restrict visibility of content;
 - limit or stop access to the service;
 - suspend or terminate someone’s account; or
 - stop someone from earning money for their content.

Recipients who receive a decision from the hosting service can bring the issue to a certified out-of-court dispute settlement body that has been certified by the [Digital Service Coordinator](#) in the Member State where the body is established.

Under Article 18 of the EMFA, VLOPs must prioritise and expedite processing and deciding complaints which are lodged by MSPs under the complaints handling systems in the [Platform-to-Business Regulation](#) (P2BR) and the DSA. MSPs may be represented by a body, such as a press council or journalists association, in the complaints-handling process.

If an MSP believes that a VLOP has repeatedly restricted or suspended its content without good reason, the VLOP must engage in “meaningful and effective dialogue” with the MSP at the MSP’s request, in order to stop current unjustified restrictions, or avoid them in the future. If no amicable solution is found following this dialogue, then the MSP may notify [the European Board of Media Services \(“Media Board”\)](#) and ask it to issue an opinion on the outcome of the dialogue, or resort to mediation or out-of-court settlement.

Do the DSA or EMFA create any specific protections for media?

The DSA and EMFA both note the importance of freedom of information, media freedom and media pluralism. While neither creates specific media privilege protections, the DSA requires intermediary services (including online platforms) to consider the impact of their actions on media freedom when moderating content or designing services. For instance, intermediary services must apply their terms and conditions with due regard to fundamental rights, including freedom and pluralism of the media.⁹ VLOPs and VLOSEs must also undertake systemic assessments of the risks stemming from the design or functioning of their service and its related systems, including risks to freedom of expression, information and pluralism of the media.¹⁰ They must take reasonable and effective measures to mitigate any identified risks.¹¹

Do the DSA or EMFA create any new transparency obligations to help identify when moderation was unfair?

The DSA sets out transparency rules for intermediary services, adds extra requirements for online platforms, and imposes further obligations on VLOPs.

All intermediary services are required to publish an annual report on content moderation that they engaged in during the relevant period. This includes reports they received of illegal content, any steps they took to moderate content due to reports or under their own initiative, and any complaints they received about this moderation. Online platforms should also include the number of – and outcomes of – out-of-court disputes with people who were unhappy with their complaint handling, and the number of users they have suspended over illegal content or unfounded complaints. VLOPs should also include information about their content moderation services, including the human resources involved, the qualifications of those people, and indicators of accuracy for any automated processes used.¹²

Online platforms must also be open about advertising by showing users who paid for an advertisement and why they are seeing it. There are additional advertising transparency obligations applicable to VLOPs; VLOPs must also undergo an independent audit at their own expense to assess their compliance with these obligations.¹³

9 Digital Services Act – Article 14(4)

10 Digital Services Act – Article 34(1)(b)

11 Digital Services Act – Article 35(1)

12 Digital Services Act – Articles 15, 24 and 42

13 Digital Services Act – Articles 26, 37 and 39

What counts as illegal content under the DSA and EMFA?

Neither the DSA nor the EMFA create new categories of illegal content. Instead, what is considered illegal is already defined in other national and EU laws. This means that content already deemed unlawful – such as hate speech, child sexual abuse material or terrorist propaganda – is treated as illegal under the DSA and EMFA.

The DSA focuses on how online platforms should respond to illegal content, requiring them to act swiftly and transparently once they are notified.

What responsibilities do digital platforms have to protect users from illegal content ?

Under the DSA, online platforms, hosting services, and VLOPs are not automatically liable for illegal content posted by users, so long as they do not have actual knowledge of the content or act quickly to remove it once they are made aware.¹⁴

It is for this reason that under Article 16 of the DSA, hosting services – including online platforms – are required to provide easy-to-use online tools for anyone – including journalists or editors – to report illegal content. These tools must enable users to submit detailed notices, including the reason why the content is suspected to be illegal, its exact location (i.e. URL), the reporter’s contact details, and the reporter’s statement confirming their good faith belief that the information and allegations in the report are accurate and complete. The hosting service must confirm receipt of a valid notice and inform the person reporting it of their decision, including how to challenge it if needed. Platforms must also suspend users who repeatedly post ‘manifestly illegal’ content.¹⁵ Under the DSA, content is considered ‘manifestly illegal’ if an ordinary person can easily tell that it breaks the law without needing expert analysis.

These rules, however, are not expected to apply to private messaging services. Private messaging services might fall within the scope of the DSA’s obligations on “mere conduit” services, but probably do not qualify as hosting services, and do not qualify as online platforms or VLOPs.

¹⁴ Digital Services Act – Article 6(1)

¹⁵ Digital Services Act – Article 23(1)

What information must a digital platform provide on how they promote or target users with content (i.e. algorithm transparency)?

Under the DSA, digital platforms, especially VLOPs and VLOSEs, must be transparent about how their algorithms promote or target content. Platforms must explain how their recommendation systems work and give users easy ways to change the settings to better suit their preferences.¹⁶ Online platforms must also include this information in their terms and conditions with users.¹⁷

VLOPs and VLOSEs must give regulators and approved researchers access to certain data, which would help monitor whether platforms are following the rules. Vetted researchers may receive access to such data only for the purpose of conducting research that contributes to identifying and understanding systemic risks and to assess risk mitigation measures.¹⁸ The European Commission is allowed under the DSA to monitor whether VLOPs and VLOSEs are following the rules, and it can request access to their data or access to the VLOP's or VLOSE's algorithm, or require an explanation of it.¹⁹ The European Commission may also appoint independent experts or auditors to help with this oversight, and non-compliance can result in fines of up to 6% of the VLOPs' or VLOSEs' global annual turnover.²⁰

Unlike the DSA, the EMFA does not impose algorithmic transparency obligations, but addresses the broader ecosystem in which media content is distributed, especially when online platforms act as gatekeepers to news and information.

What do VLOPs and VLOSEs need to include in their risk assessments?

Under Article 34 of the DSA, VLOPs and VLOSEs must regularly assess risks linked to how their services are designed, how their algorithms work, and how people use their services. The risk assessment must be carried out at least annually, and also before launching new features that are likely to have a critical impact on the risks identified. The assessment must include the following “systemic risks”:

- the dissemination of illegal content through their services;
- any actual or foreseeable negative effects on fundamental rights – including the right to privacy and freedom of expression and information, which includes the freedom and pluralism of the media;

¹⁶ Digital Services Act – Article 27

¹⁷ Digital Services Act – Article 14

¹⁸ Digital Services Act – Article 40

¹⁹ Digital Services Act – Articles 40 and 72

²⁰ Digital Services Act – Articles 52(3) and 72(2)

- any actual or foreseeable negative effects on civic discourse, electoral processes, or public security; and
- any actual or foreseeable negative effects on gender-based violence, the protection of public health and minors, or serious negative consequences to a person's physical and mental well-being.

When conducting assessments of the systemic risks, providers of VLOPs and VLOSEs must consider how the following features contribute to such risks:

- the design of their recommendation algorithms;
- their content moderation systems;
- the terms and conditions and their enforcement;
- systems for selecting and presenting advertisements; and
- data related practices of the provider.

Providers of VLOPs and VLOSEs must also consider how quickly and widely such content can spread on their platforms. After they identify systemic risks, Article 35 requires VLOPs and VLOSEs to take action to reduce them. These actions should be reasonable, proportionate, and tailored to the specific problems found. Examples of actions VLOPs and VLOSEs may take include improving content moderation, adjusting algorithms, changing how advertisements are shown, working with trusted flaggers, and protecting children online.

Under Article 27, providers of VLOPs and VLOSEs must undergo independent audits, and the organisation performing an audit must issue a report. Within three months of the audit report, providers of VLOPs and VLOSEs must publish the audit report, a report summarising the risk assessments undertaken under Article 34, and the specific measures put in place to address those risks under Article 35, in addition to other relevant information.

Is there a process for stakeholders to work with regulators on the content of risk assessments?

The DSA does not set out a formal process for how stakeholders may work with regulators on the content of risk assessments. However, there are a number of ways stakeholders may still be involved:

- **Engaging with VLOPs and VLOSEs when conducting risk assessments:** The DSA encourages VLOPs and VLOSEs to involve their users, civil society groups, and independent experts when assessing risks and deciding how to reduce them. VLOPs

and VLOSEs should use methods like surveys, focus groups, and roundtables to gather input.²¹

- **Engaging with the European Commission on guidelines on mitigating risks:** The European Commission is required under the DSA to hold public consultations when preparing guidelines that help platforms understand how to reduce specific risks. These guidelines can include best practices and recommended actions, and must consider how these actions affect fundamental rights.²²
- **Engaging with the European Commission on voluntary codes of conduct for major risks:** The European Commission can invite VLOPs, VLOSEs, and other online services, civil society organisations, and regulators to help create voluntary codes of conduct if a serious risk arises that affects multiple platforms. These codes may include commitments to take specific actions, report regularly on what has been done, and share the results of those efforts.²³

What powers do regulators have to require platforms to take specific actions after a risk assessment?

The DSA does not grant the European Commission a specific power to require VLOP providers to take specific mitigation measures in response to the risks they identify in their risk assessments. However, the Commission can publish guidelines that share best practices and recommend possible measures for VLOPs and VLOSEs to reduce risks.²⁴ It must also encourage and facilitate the drawing up of voluntary codes of conduct that set out commitments to take specific risk mitigation measures.²⁵ The Board, in cooperation with the Commission, is also obliged to publish annual reports that include information on the most common risks identified or reported and recommend best practices to address them.²⁶ If the Commission believes that a VLOP or VLOSE provider has broken the rules on risk assessments and mitigation measures or any other provisions, it may issue requests for information, conduct interviews and carry out inspections.²⁷ If the situation is urgent and could seriously harm users, the Commission can order the VLOP or VLOSE provider to take interim steps to address the risk.²⁸ If, in the context of an investigation, a VLOP or VLOSE makes commitments to ensure compliance the Commission can make those commitments binding and declare there are no further grounds for action, and if the Commission finds an infringement, it can issue fines for non-compliance.²⁹

21 Digital Services Act – Recital 90

22 Digital Services Act – Article 35(3)

23 Digital Services Act – Article 45(1)

24 Digital Services Act – Article 35(3)

25 Digital Services Act – Article 45(1)

26 Digital Services Act – Article 35(2)

27 Digital Services Act – Articles 34, 35, 67, 68 and 69

28 Digital Services Act – Article 70(1)

29 Digital Services Act – Article 70(1) and 74

What rights do media organisations have to bring complaints to regulators and/or submit evidence?

Under the DSA, media organisations, as users of intermediary services, have the right to lodge a complaint with the Digital Services Coordinator (DSC) in the country where they are based.³⁰ These complaints may help regulators understand concerns about how platforms follow the rules. The DSC in that country must assess the complaint and, where appropriate, send the complaint to the DSC in the country where the platform is based, possibly with comments. During complaint proceedings, both sides – the person or group making the complaint and the platform – have the right to share their views and get updates on the status of the complaint, in accordance with national laws.

The EMFA does not set out a specific enforcement system for how VLOPs must follow its rules. However, if an MSP has a “dialogue” with a VLOP, on the grounds that the VLOP has repeatedly and without good reason restricted the MSP’s content, the MSP can report the outcome to the European Board for Digital Services and the European Commission. The MSP can also ask the Board to give its opinion on the outcome, including suggestions for what the platform should do next. The Board must then share its opinion with the Commission.³¹

Under the EMFA, the European Commission may take these opinions into account when enforcing the DSA. This means that while the EMFA does not directly enforce rules on platforms, it creates a way for concerns to be raised and potentially influence how the DSA is applied.

³⁰ Digital Services Act – Article 53

³¹ European Media Freedom Act – Article 18(6)



View of the European Parliament in Strasbourg, France June 12, 2023. REUTERS/Yves Herman

DSA & EMFA Risk Checklist for Media

1. Confirm MSP Status & Eligibility

- ☐ Verify your activities qualify as “media services” and you qualify as a “media service provider” (MSP).
- ☐ Self-declare MSP status to Very Large Online Platforms (VLOPs) to obtain EMFA safeguards:
 - ☐ Confirm you provide to your users your: legal name, contact details, full ownership details, beneficial ownership, public/state advertising revenues, third country advertising revenues.
 - ☐ Confirm editorial independence from governments, political parties, third country entities.
 - ☐ Show compliance with national law of an EU country or recognised self/co-regulatory standards.
 - ☐ Confirm AI-generated content receives human editorial review.
 - ☐ Declare the contact details of the relevant oversight bodies for your editorial standards.
 - ☐ Contact details the provider can use to contact you directly and quickly.

2. Manage Content Moderation Risk

- ☐ Review platform moderation rules, which they are required to have in their terms and conditions.
- ☐ Review the platform's annual reports on the moderations actions they have taken in the previous year.
- ☐ Expect specific reasons for any restriction/removal, including legal basis, rule breached, duration, and any automation used.
- ☐ Use the **24-hour notice period** before VLOPs restrict your content (unless the content is illegal).

3. Use Redress & Complaints Rights

- ☐ Use platforms' internal complaint systems (which are required to be free and have a six-month window to raise complaints).
- ☐ Expect priority handling of MSP complaints, and approach the VLOP for "meaningful and effective dialogue" if your services are repeatedly restricted.
- ☐ Consider whether you would like to approach a body, such as a press council or journalists association, to represent you in the complaint procedure.
- ☐ Consider reporting the outcomes of "meaningful ... dialogues" with VLOPs to the European Board for Media Services.
- ☐ If no amicable solution is found, consider mediation or out of court settlement.
- ☐ If you have broader complaints about how a platform is conducting itself, lodge a complaint with the Digital Services Coordinator (DSC) in the country in which you are based.

4. Engage With VLOPs Proactively

- ☐ Review VLOP/Very Large Online Search Engine (VLOSE) annual systemic risk assessments and published summaries.
- ☐ Participate in stakeholder consultations with VLOPs, VLOSEs and the European Commission where possible.

Disclaimer

This Guide is offered for information purposes only. It is not legal advice. Readers are urged to seek advice from qualified legal counsel in relation to their specific circumstances. We intend the Guide's contents to be correct and up to date at the time of publication, but we do not guarantee their accuracy or completeness, particularly as circumstances may change after publication. The Thomson Reuters Foundation accept no liability or responsibility for actions taken or not taken or any losses arising from reliance on this Guide or any inaccuracies herein.

About Us

The [Thomson Reuters Foundation](#) is the corporate foundation of Thomson Reuters, the global news and information services company. As an independent charity, registered in the UK and the USA, we leverage our media, legal and data-driven expertise to strengthen independent journalism, enable access to the law and promote responsible business. Through news, media development, free legal assistance and data intelligence, we aim to build free, fair and informed societies.

TrustLaw, an initiative of the Thomson Reuters Foundation, is the world's largest pro bono legal network. Working with leading law firms and corporate legal teams, we facilitate free legal support, ground-breaking legal research and resources for non-profits, independent media and social enterprises in over 190 countries. By spreading the practice of pro bono worldwide, TrustLaw wants to strengthen civil society and drive change. If you have ideas for resources we could develop or [legal research projects](#) that would be of assistance after reading this guide, please [contact us](#). If you are a non-profit or social enterprise in need of legal support, you can find out more about the service [here](#) and join [TrustLaw](#) for free.

The Thomson Reuters Foundation's global pro bono legal network, TrustLaw, works with leading law firms and corporate legal teams to facilitate free legal support, research, and resources for civil society organisations, social enterprises, and non-profit independent media around the globe.

For more information, visit www.trust.org.

TrustLaw

