

Wie Hosting-Service-Provider ihren Beitrag zur Bekämpfung terroristischer Inhalte auf ihren Plattformen optimieren

Ein sechs-stufiger Leitfaden zur Umsetzung der europäischen TCO-Verordnung

Sophia Rothut, Heidi Schulze, Diana Rieger,
Catherine Bouko und Brigitte Naderer



Tech Against Terrorism Europe (TATE)

Dieser Leitfaden ist Teil von Tech Against Terrorism Europe (TATE). Das TATE-Projekt wird von der Europäischen Union finanziert (ISF-2021-AG-TCO-101080101). Dieses Projekt unterstützt kleinere Anbieter von Hosting-Diensten (Hosting-Service-Provider; HSPs) beim Aufbau notwendiger Rahmenbedingungen und Maßnahmen für die Terrorismusbekämpfung und bei der Transparenzberichterstattung, wie in der EU-Verordnung zur Bekämpfung der Verbreitung terroristischer Online-Inhalte (engl.: Terrorist Content Online; TCO) und in der Richtlinie (EU) 2017/541 gefordert.

tate.techagainterrorism.org



Finanziert von der
Europäischen Union

Autorinnen

Sophia Rothut ist wissenschaftliche Mitarbeiterin am Lehrbereich von Prof. Dr. Rieger (IfKW, LMU München). Im Rahmen des EU-Projekts TATE arbeitet sie an den Voraussetzungen für die Bekämpfung terroristischer Inhalte im Internet. Ihre Forschungsschwerpunkte liegen in den Bereichen Online-Radikalisierung, Mainstreaming und politische/Rechtsaußen-Influencer:innen

Heidi Schulze ist wissenschaftliche Mitarbeiterin am Institut für Kommunikationswissenschaft und Medienforschung an der LMU München. An der LMU ist sie Teil des Lehrbereichs von Prof. Dr. Rieger und untersucht Radikalisierungsdynamiken im Internet im Rahmen des groß angelegten interdisziplinären Spitzenforschungsclusters MOTRA – Monitoringsystem und Transferplattform Radikalisierung. In ihrer Forschung konzentriert sie sich auf radikale/extremistische (Gruppen-) Kommunikation auf alternativen sozialen Plattformen und Fringe Communities sowie auf die Eigenschaften und das Publikum von hyperpartisanen Nachrichten-Webseiten.

Diana Rieger ist Professorin am Institut für Kommunikationswissenschaft und Medienforschung (IfKW) and der Ludwig-Maximilians-Universität München (LMU). Sie forscht zu Online-Radikalisierung, Hassrede und den Auswirkungen von Unterhaltungsinhalten. Darüber hinaus beschäftigt sie sich mit der Entwicklung und Evaluierung von Gegenmaßnahmen gegen Radikalisierung.

Catherine Bouko ist außerordentliche Professorin für Kommunikation und Französisch an der Universität Gent (Belgien). Ihr Forschungsschwerpunkt liegt auf politischer Kommunikation, Extremismus und der Gesellschaft in sozialen Medien, mit einem besonderen Fokus auf bildbasierte Kommunikation. Zu ihren Forschungsmethoden gehören (multimodale) Diskursanalyse, quantitative Inhaltsanalyse, Semiotik und Ethnographie.

Brigitte Naderer ist wissenschaftliche Mitarbeiterin (Post-Doc) an der Medizinischen Universität Wien im Zentrum für Public Health, Abteilung für Sozial- und Präventivmedizin, Abteilung Suizidforschung & Psychische Gesundheitsförderung und war bis März 2023 am Institut für Medien und Kommunikation (LMU München) tätig. Ihre Forschungsschwerpunkte sind Medienkompetenz, Online-Radikalisierung und Medienwirkungen auf Kinder und Jugendliche.

Danksagung: Wir danken Tech Against Terrorism für ihren Input und ihr Feedback zu diesem Leitfaden. Außerdem möchten wir Professor Maura Conway für ihre hilfreichen Kommentare danken.

Inhaltsverzeichnis

A. Einleitung	4
B. Zentrale Verpflichtungen und Empfehlungen in Bezug auf die TCO-Verordnung.....	8
Kapitel 1 Erarbeitung von Nutzungsbedingungen zum Verbot terroristischer Inhalte	10
1. Was sind Nutzungsbedingungen?.....	11
2. Warum ist es notwendig, klare und robuste Nutzungsbedingungen zu haben?	11
3. Praktische Tipps und Ratschläge: Was sind Elemente robuster Nutzungsbedingungen?	12
Kapitel 2 Spezifische Maßnahmen zur Identifizierung und Entfernung von (terroristischen) Inhalten	15
1. Warum ist es notwendig, Identifizierungsprozesse für illegale und schädliche Inhalte einzuführen?	16
2. Ein Prozess zur Identifizierung terroristischer Inhalte	16
3. Praktische Tipps und Ratschläge: Was hilft bei der Beurteilung, ob ein Inhalt illegal ist?	18
4. Was soll ich tun, wenn ich es anders sehe? Eine erhaltene Entfernungsanordnung anfechten	21
Kapitel 3 Etablierung wirksamer Moderationsmechanismen für terroristische Online-Inhalte	22
1. Was ist Inhaltsmoderation und warum ist sie in manchen Fällen notwendig?	22
2. Praktische Tipps und Ratschläge: Welche Verfahren der Inhaltsmoderation kommen in Frage?	25
3. Alternative Moderationsansätze	27
Kapitel 4 Einrichtung von Kontaktstellen und gesetzlichen Vertreter:innen	29
1. Was sind Kontaktstellen und gesetzliche Vertreter:innen?	29
2. Warum ist eine Kontaktstelle oder ein:e gesetzliche:r Vertreter:in notwendig?	30
3. Was ist die zuständige Behörde eines EU-Mitgliedstaates und wie kann ich mit ihr Kontakt aufnehmen?	31
Kapitel 5 Aufbau eines Benachrichtigungs- und Beschwerdesystems für entfernte Inhalte	32
1. Warum ist es notwendig, einen transparenten Beschwerdemechanismus einzurichten?	32
2. Was sind die Anforderungen an ein Beschwerdesystem?	33
3. Wie wird mit Beschwerden umgegangen und was sind die möglichen Folgen?	33
4. Praktische Tipps und Ratschläge: Welche Elemente sind beim Aufbau eines Beschwerdesystems sinnvoll?	34
Kapitel 6 Praktische Unterstützung und Ratschläge zur Transparenzberichterstattung	36
1. Was sind Transparenzberichte?.....	36
2. Warum sind Transparenzberichte notwendig?.....	37
3. Ein Prozess für die Erstellung von Transparenzberichten	38
4. Welche Informationen und Kennzahlen müssen gemäß TCO-Verordnung in den Transparenzbericht aufgenommen werden?.....	40
C. Vielen Dank für Ihre Hilfe bei der Bekämpfung der terroristischen Bedrohung!.....	41
D. Glossar	42

A. Einleitung

Worum es in diesem Leitfaden geht, und warum Sie ihn lesen sollten ...

Dieser Leitfaden befasst sich mit den **Verpflichtungen, die den Hosting-Service-Providern (HSP) durch die europäische Verordnung zur Bekämpfung der Verbreitung terroristischer Online-Inhalte von April 2021 auferlegt werden**. Diese Verordnung wird, abgeleitet von der Abkürzung *TCO*, die für den englischen Begriff Terrorist Content Online (dt.: terroristische Online-Inhalte) steht, in der Praxis meist als **TCO-Verordnung** bezeichnet.

Der Leitfaden befasst sich mit der Frage, was HSPs berücksichtigen müssen, um der Verbreitung terroristischer Inhalte im Internet entgegenzuwirken, und gibt praktische Ratschläge für die Umsetzung verschiedener Maßnahmen.

Der Leitfaden konzentriert sich zum einen auf die **Mindestanforderungen, die HSPs erfüllen müssen, um die TCO-Verordnung einzuhalten**. Zweitens enthält er **Tipps und praktische Ratschläge zu den relevanten (pro-)aktiven Maßnahmen, die HSPs ergreifen sollten**, um die Komplexität der Rechtsdurchsetzung erfolgreich zu bewältigen (z. B. was zu tun ist, wenn eine Entfernungsanordnung in Ihrer Mailbox landet) und um HSPs darauf vorzubereiten, der terroristischen Vereinnahmung ihrer Plattformen entgegenzuwirken.

Der Leitfaden ist Teil des von der Europäischen Union finanzierten Projekts [Tech Against Terrorism Europe \(TATE\)](#). Das TATE-Konsortium besteht aus der Dublin City University, der Universität Gent, dem JOS-Projekt, der Ludwig-Maximilians-Universität München, Saher Europe, der Swansea University und Tech Against Terrorism. Ziel von TATE ist es, das Bewusstsein für die TCO-Verordnung der EU zu schärfen und kleine(re) HSPs dabei zu unterstützen, Maßnahmen zur Einhaltung und Unterstützung der TCO-Verordnung zu ergreifen. Zusammen mit anderen Ressourcen hat TATE diesen Leitfaden erstellt, um die rechtlichen und praktischen Erwartungen für HSPs so greifbar wie möglich zu machen.

Für wen ist dieser Leitfaden gedacht?

Der Leitfaden richtet sich an Anbieter von Internetdienstleistungen (Hosting-Service-Provider; HSP) und ihre Mitarbeiter:innen sowie an IT-Fachkräfte, die technische Funktionen zur Bekämpfung terroristischer Inhalte in die Plattformarchitekturen implementieren wollen und/oder müssen. Er soll über die Mindestanforderungen informieren, die erfüllt werden müssen, um die TCO-Verordnung der EU von 2021 (29. April) einzuhalten.

Wir haben diesen Leitfaden und andere TATE-Ressourcen erstellt, um kleine(re) HSPs zu unterstützen. Gerade kleine(re) HSPs haben oft nur begrenzte Ressourcen, um gegen terroristische Inhalte auf ihren Plattformen vorzugehen. Daher möchten wir diese gerne besonders unterstützen. Es ist nämlich **von entscheidender Bedeutung, dass kleine(re) HSPs die Bedrohung durch terroristische Inhalte nicht vernachlässigen, da kleinere Plattformen eher von terroristischen Akteur:innen ausgenutzt werden können** (weitere dazu finden Sie in [diesem Bericht über Tech Against Terrorism](#)).

Was sind die Kernelemente der TCO-Verordnung?

Die [europäische Verordnung zur Bekämpfung der Verbreitung terroristischer Online-Inhalte \(TCO-Verordnung\)](#) ist im Juni 2022 in Kraft getreten und **verpflichtet Internetdienstleister, innerhalb einer Stunde nach Erhalt einer Entfernungsanordnung von einer zuständigen Behörde, die entsprechenden Inhalte zu entfernen oder den Zugang zu ihnen zu sperren.**

HSPs müssen mit Strafverfolgungsbehörden wie Europol und anderen zuständigen Behörden zusammenarbeiten, um terroristische Inhalte auf ihren Plattformen zu erkennen und zu entfernen. Um die TCO-Verordnung einzuhalten, **müssen die Diensteanbieter außerdem wirksame und verhältnismäßige Maßnahmen ergreifen, um zu verhindern, dass terroristische Inhalte erneut hochgeladen werden**, und sie haben weitere Verpflichtungen, die Sie in diesem Leitfaden kennenlernen werden.

Wie ist dieser Leitfaden aufgebaut?

Im Zuge der TCO-Verordnung werden HSPs derzeit dazu verpflichtet und angehalten,...

- 1) ...angemessene Nutzungsbedingungen auszuarbeiten (► [Kapitel 1](#)),
- 2) ...spezifische Maßnahmen zur Erkennung und Entfernung terroristischer Inhalte zu ergreifen (► [Kapitel 2](#)),
- 3) ...wirksame Moderationsmechanismen zu etablieren (► [Kapitel 3](#)),
- 4) ...Kontaktstellen und gesetzliche Vertreter:innen einzurichten (► [Kapitel 4](#)),
- 5) ...Benachrichtigungs- und Beschwerdemechanismen für ihre Nutzer:innen aufzubauen (► [Kapitel 5](#)),
- 6) ...Transparenzberichte zu verfassen (► [Kapitel 6](#)).

Wir haben die Erläuterungen und Empfehlungen in diesem Leitfaden nach diesen sechs Hauptanforderungen gegliedert. Zu Beginn eines jeden Kapitels finden Sie eine kurze Zusammenfassung der Inhalte und der wichtigsten Punkte des jeweiligen Kapitels. Danach erhalten Sie ausführliche Informationen darüber, was die TCO-Verordnung von den HSPs verlangt und was sie Ihnen darüber hinaus dringend nahelegt, sowie weitere praktische Ratschläge zum Schutz Ihrer Plattform vor terroristischen (und anderen schädlichen) Inhalten.

Welche Plattformen sind von der TCO-Verordnung betroffen?

Die TCO-Verordnung betrifft Hosting-Dienst-Provider (HSPs), d. h. alle Plattformen, die es Nutzer:innen ermöglichen, über ihre Dienste Informationen an die Öffentlichkeit zu verbreiten.

Die TCO-Verordnung gilt für **HSPs jeder Größe und für jeden HSP, der seine Dienste in der EU anbietet**. Sie gilt auch für HSPs mit Sitz außerhalb der EU, wenn ein HSP (1) eine erhebliche Anzahl von Nutzer:innen in einem oder mehreren EU-Mitgliedstaaten hat oder (2) seine Aktivitäten auf einen oder mehrere EU-Mitgliedstaaten ausrichtet.

Wann gilt ein HSP als „terroristischen Inhalten ausgesetzt“?

Die TCO-Verordnung erlegt HSPs, die „terroristischen Inhalten ausgesetzt sind“, besondere Verpflichtungen auf. Gemäß [Art. 5.4](#) ist ein HSP dann terroristischen Inhalten ausgesetzt, wenn er in den vergangenen 12 Monaten von der zuständigen Behörde des Mitgliedstaats, in dem der HSP seine Hauptniederlassung oder seine:n gesetzliche:n Vertreter:in in der EU hat, über zwei oder mehr endgültige Entfernungsanordnungen informiert wurde und diese erhalten hat.

Was sind terroristische Inhalte?

Da es in der TCO-Verordnung um terroristische Inhalte geht, die online verbreitet werden, ist es zuerst wichtig, diese zu definieren. Die [EU-Richtlinie 2017/541](#) legt die Grundlage für die TCO-Verordnung, indem sie definiert, was als terroristischer Inhalt zu verstehen ist.

Inhalte werden als terroristisch eingestuft, wenn sie zu Handlungen anstiften oder Absichten zugunsten einer terroristischen Sache fördern und damit direkt oder indirekt zur Gefahr terroristischer Straftaten beitragen.

Die Androhung einer terroristischen Straftat gilt ebenfalls als terroristischer Inhalt, ebenso wie die Bereitstellung von Informationen, Unterstützung oder Finanzierung für diese Handlungen.

Arten von terroristischen Straftaten

Zu den terroristischen Straftaten können unter anderem folgende Straftaten gehören ([EU-Richtlinie 2017/541, Art. 3.1](#)):

- Angriffe auf das Leben oder die körperliche Unversehrtheit einer Person
- Entführung oder Geiselnahme
- weitreichende Zerstörungen an bestimmten Einrichtungen und Infrastrukturen (z. B. staatliche/öffentliche Einrichtungen, Verkehrs- und Informationssysteme), die Menschenleben gefährden oder zu großen wirtschaftlichen Verlusten führen können
- Kaperung von Flugzeugen, Schiffen, anderen öffentlichen Verkehrsmitteln oder Gütertransportmitteln
- Herstellung, Besitz, Erwerb, Beförderung, Bereitstellung oder Verwendung von Sprengstoffen oder Waffen sowie Forschung und Entwicklung von chemischen, biologischen, radiologischen oder atomaren Waffen
- Freisetzung gefährlicher Stoffe oder Verursachung von Bränden, Überschwemmungen oder Explosionen
- Beeinträchtigung oder Unterbrechung der Versorgung mit Wasser, Strom oder anderen grundlegenden natürlichen Ressourcen, durch die menschliches Leben gefährdet wird.

Die Leitung einer terroristischen Vereinigung oder die vorsätzliche Beteiligung an deren Aktivitäten wird ebenfalls als Straftat betrachtet ([EU-Richtlinie 2017/541, Art. 4](#)). Dazu gehört auch die Bereitstellung von (Informations-)Ressourcen (z. B. Anweisungen oder Materialien zum Bau von Waffen) für terroristische Zwecke oder die Finanzierung solcher Aktivitäten.

Mit solchen Straftaten zielen terroristische Akteure darauf ab, (a) die Bevölkerung einzuschüchtern, (b) öffentliche Akteur:innen oder eine internationale Organisation in unzulässiger Weise dazu zu zwingen, eine bestimmte Handlung (nicht) auszuführen, oder (c) die grundlegenden verfassungsrechtlichen, politischen, wirtschaftlichen oder sozialen Strukturen eines Landes oder einer internationalen Organisation ernsthaft zu destabilisieren oder zu zerstören ([EU-Richtlinie 2017/541, Art. 3.2](#)).



Zusammenfassend lässt sich sagen, dass Inhalte als terroristische Inhalte gelten, wenn sie eine terroristische Straftat ermöglichen, unterstützen oder erleichtern oder wenn sie eine Drohung zur Begehung einer terroristischen Straftat enthalten.

B. Zentrale Verpflichtungen und Empfehlungen in Bezug auf die TCO-Verordnung

In den folgenden Kapiteln finden Sie Informationen über sechs Schlüsselkomponenten und Schritte, um Ihre Plattform gegen die terroristische Bedrohung zu rüsten. Dazu gehören die folgenden Kernbereiche und Fragen.

Kapitel 1: Erarbeitung von Nutzungsbedingungen zum Verbot terroristischer Inhalte

1. Was sind Nutzungsbedingungen?
2. Warum ist es notwendig, klare und robuste Nutzungsbedingungen zu haben?
3. Praktische Tipps und Ratschläge: Was sind Elemente robuster Nutzungsbedingungen?

Kapitel 2: Spezifische Maßnahmen zur Identifizierung und Entfernung von (terroristischen) Inhalten

1. Warum ist es notwendig, Identifizierungsprozesse für illegale und schädliche Inhalte einzuführen?
2. Ein Prozess zur Identifizierung terroristischer Inhalte
3. Praktische Tipps und Ratschläge: Was hilft bei der Beurteilung, ob ein Inhalt illegal ist?
4. Was soll ich tun, wenn ich es anders sehe? Eine erhaltene Entfernungsanordnung anfechten

Kapitel 3: Etablierung wirksamer Moderationsmechanismen für terroristische Online-Inhalte

1. Was ist Inhaltsmoderation und warum ist sie in manchen Fällen notwendig?
2. Praktische Tipps und Ratschläge: Welche Verfahren der Inhaltsmoderation kommen in Frage?
3. Alternative Moderationsansätze

Kapitel 4: Einrichtung von Kontaktstellen und gesetzlichen Vertreter:innen

1. Was sind Kontaktstellen und gesetzliche Vertreter:innen?
2. Warum ist eine Kontaktstelle oder ein:e gesetzliche:r Vertreter:in notwendig?
3. Was ist die zuständige Behörde eines EU-Mitgliedstaats und wie kann ich mit ihr Kontakt aufnehmen?

Kapitel 5: Aufbau eines Benachrichtigungs- und Beschwerdesystems für entfernte Inhalte

1. Warum ist es notwendig, einen transparenten Beschwerdemechanismus einzurichten?
2. Was sind die Anforderungen an ein Beschwerdesystem?
3. Wie wird mit Beschwerden umgegangen und was sind die möglichen Folgen?
4. Praktische Tipps und Ratschläge: Welche Elemente sind beim Aufbau eines Beschwerdesystems sinnvoll?

Kapitel 6: Praktische Unterstützung und Ratschläge zur Transparenzberichterstattung

1. Was sind Transparenzberichte?
2. Warum sind Transparenzberichte notwendig?
3. Ein Prozess für die Erstellung von Transparenzberichten
4. Welche Informationen und Kennzahlen müssen gemäß TCO-Verordnung in den Transparenzbericht aufgenommen werden?

Der Leitfaden erläutert die **Aspekte der TCO-Verordnung, die für die Plattformen verpflichtend sind** und gibt gleichzeitig **praktische Ratschläge für proaktive Maßnahmen, die ergriffen werden können, um die Verbreitung schädlicher Inhalte im Internet zu verhindern**. Solche Maßnahmen sind unerlässlich, um Plattformen gegen die terroristische Ausnutzung ihrer Dienste zu wappnen – oder in der Sprache der TCO-Verordnung: um mit der Situation umgehen zu können, wenn die erste und jede weitere Entfernungsanordnung in Ihrer Mailbox landet.

Kapitel 1

Erarbeitung von Nutzungsbedingungen zum Verbot terroristischer Inhalte



Zusammenfassung: Inhalt und Kernpunkte dieses Kapitels

- Die Nutzungsbedingungen sind eine **verbindliche Vereinbarung** zwischen den Nutzer:innen und dem HSP, in der die angemessene und zulässige Nutzung der Plattform festgelegt ist.
- HSPs müssen (1) ihre **Strategie zur Bekämpfung der Verbreitung terroristischer Inhalte** in ihren Nutzungsbedingungen darlegen und (2) die Verbreitung **terroristischer Inhalte verbieten**.
- Über den Geltungsbereich der TCO-Verordnung hinaus können und sollten HSPs in Erwägung ziehen, auch andere Formen schädlicher Inhalte (z. B. extremistische Inhalte, Hassrede) zu verbieten.
- Nutzungsbedingungen sind eine **rechtliche Notwendigkeit** im Rahmen der TCO-Verordnung und stellen auch eine **nützliche Schutzmaßnahme für die Plattform** dar.
- Es sind mehrere Elemente erforderlich, um Ihre Nutzungsbedingungen so robust wie möglich zu gestalten. Dazu gehören unter anderem die Definition von terroristischen Inhalten sowie die Offenlegung der Strategie zur Bekämpfung terroristischer Inhalte auf der jeweiligen Plattform.

Geeignete **Nutzungsbedingungen** sind **die Grundlage für das Verbot terroristischer Inhalte und den entsprechenden Umgang damit**. Die TCO-Verordnung fordert HSPs ausdrücklich auf, dass HSPs „in ihren Nutzungsbedingungen deutlich ihre Strategie zur Bekämpfung der Verbreitung terroristischer Inhalte dar[legen], gegebenenfalls mit einer aussagekräftigen Erläuterung der Funktionsweise spezifischer Maßnahmen, gegebenenfalls einschließlich der Verwendung automatisierter Verfahren“ ([TCO-Verordnung, Art. 7.1](#)).

Zusätzlich, und über den Anwendungsbereich der TCO-Verordnung hinaus, können und sollten HSPs erwägen, auch **andere Formen von schädlichen Inhalten** (z. B. extremistische Inhalte, Hassrede, Befürwortung von Gewalt) in ihren Nutzungsbedingungen zu verbieten. Auf diese Weise können HSPs zur Schaffung eines Rahmens für eine zivile digitale Diskurskultur beitragen.

1. Was sind Nutzungsbedingungen?

Nutzungsbedingungen sind Regeln, die von und für die jeweilige Plattform aufgestellt werden und die (1) die Verantwortung des HSPs gegenüber seinen Nutzer:innen und (2) angemessene und erlaubte, aber auch verbotene Inhalte und Verhaltensweisen auf dieser Plattform festlegen. Die Nutzer:innen müssen die Nutzungsbedingungen akzeptieren, wenn sie den von dem HSP angebotenen Dienst in Anspruch nehmen wollen.

Im Englischen werden Nutzungsbedingungen häufig als Terms of Service (abgekürzt: ToS) bezeichnet. Es gibt aber auch weitere Begriffe, wie Terms of Use, Terms and Conditions oder Community Standards, die synonym dazu genutzt werden. Die TCO verwendet im Deutschen den Begriff „Nutzungsbedingungen“ und im Englischen den Begriff „Terms and Conditions“ und definiert diese als „sämtliche Bestimmungen, Bedingungen und Klauseln, unabhängig von ihrer Bezeichnung oder Form, zur Regelung der vertraglichen Beziehungen zwischen einem Hostingdiensteanbieter und seinen Nutzern“ ([TCO-Verordnung, Art. 2.8](#)).

2. Warum ist es notwendig, klare und robuste Nutzungsbedingungen zu haben?

Um einen tieferen Einblick in die Frage zu erhalten, warum klare und robuste Nutzungsbedingungen notwendig sind, nehmen wir zwei verschiedene Perspektiven ein: die rechtliche und die unternehmerische/operative.

a) Rechtliche Perspektive

Einhaltung von (EU-)Gesetzen

Nutzungsbedingungen müssen dem aktuellen (EU-)Recht entsprechen, einschließlich der TCO-Verordnung, aber auch der [EU-Richtlinie 2017/541](#), die den EU-weiten Umgang mit terroristischen Inhalten stärkt, indem sie (1) eine Definition terroristischer Inhalte liefert, (2) Strafen für diese festlegt ([Art. 15](#)), (3) die Rechte und die Unterstützung der Opfer stärkt und (4) Terrorismus als transnationale, grenzüberschreitende Bedrohung anerkennt. Sowohl diese Richtlinie als auch die TCO-Verordnung fördern die EU-weite und internationale Zusammenarbeit. Die Nutzungsbedingungen sind ein Ort, an dem der HSP sein Engagement für die Bekämpfung terroristischer Aktivitäten hervorheben kann.

Schutz des HSPs vor rechtlicher Haftung

Die Nutzungsbedingungen sollen den HSP vor Haftung schützen (sofern diese im Rahmen des geltenden Rechts liegen). Da es sich um einen Vertrag zwischen dem HSP und seinen Nutzer:innen handelt, sind die Nutzungsbedingungen eine rechtsverbindliche Vereinbarung zwischen diesen beiden Parteien. Nutzungsbedingungen ermöglichen es dem HSP, Regeln für die (nicht) akzeptierte Nutzung im Einklang mit den Werten des HSPs festzulegen.

Grundlage für die (proaktive) Entfernung von Inhalten

Darüber hinaus sind klare Nutzungsbedingungen wichtig, wenn es um problematische Inhalte und deren Moderation geht. HSPs können sich auf ihre Nutzungsbedingungen berufen, um die Moderation von Inhalten zu rechtfertigen, wenn sie detaillierte Informationen über verbotene Inhaltspraktiken, einschließlich eines Terrorismusverbots, enthalten.

b) Perspektive des Unternehmens

Aufrechterhaltung des operativen Geschäfts

Erstens ist es für den Fortbestand des operativen Geschäfts und damit für den Erfolg des Unternehmens von zentraler Bedeutung, die Rechtsvorschriften einzuhalten. HSPs haben eine gewisse Verantwortung gegenüber ihrer Stakeholder, die die Einhaltung geltender Vorschriften erwarten. Darüber hinaus kann es zu einer finanziellen Haftung kommen und Strafen oder Rufschädigung sind weitere mögliche Folgen der Nichteinhaltung.

Demonstration der öffentlichen Verantwortung der HSP

Zweitens haben HSPs als zentrale gesellschaftliche Akteure eine Verantwortung gegenüber der Öffentlichkeit, sowohl auf kollektiver als auch auf individueller Basis. Die Verantwortung gegenüber der breiten Öffentlichkeit besteht darin, illegale Aktivitäten wie Terrorismus zu bekämpfen und terroristische Inhalte zu erkennen und zu verhindern, bevor sie weit verbreitet werden. Indem sie in den Nutzungsbedingungen festhalten, dass illegale Aktivitäten verboten sind, legen HSPs eine Grundlage für eine sicherere Online-Sphäre und können sich darauf zurückbeziehen, wenn sie gegen (illegale) Inhalte vorgehen. Klare Nutzungsbedingungen helfen den HSPs auch, ihre Verantwortung gegenüber den einzelnen Mitgliedern der Öffentlichkeit zu demonstrieren, indem sie durch Transparenz Vertrauen schaffen. In dieser Hinsicht zeigen HSPs den einzelnen Nutzer:innen, dass sie vor schädlichen Inhalten auf der Plattform geschützt werden sollen, wenn solche Inhalte in den Nutzungsbedingungen ausdrücklich verboten sind.

3. Praktische Tipps und Ratschläge: Was sind Elemente robuster Nutzungsbedingungen?

In den folgenden Abschnitten finden Sie Hinweise zu den Elementen, die Sie als HSP bei der Erstellung von Nutzungsbedingungen im Zusammenhang mit der TCO-Verordnung berücksichtigen sollten.

Es ist wichtig zu betonen, dass die Entwicklung von Nutzungsbedingungen ein iterativer Prozess ist: Die Nutzungsbedingungen können und sollten bei Bedarf angepasst werden, z. B. als Reaktion auf Vorschläge von Nutzer:innen und um mit der Entwicklung nationaler oder internationaler Rechtsvorschriften Schritt zu halten. Die TCO-Verordnung fordert eine solche Anpassungsfähigkeit: HSPs müssen, wenn sie terroristischen Inhalten ausgesetzt sind, ihre Nutzungsbedingungen dahingehend ändern, dass sie darauf hinweisen und **darlegen, welche Maßnahmen ergriffen werden, um dem Missbrauch der Plattform für terroristische Zwecke entgegenzuwirken** ([TCO-Verordnung, Art. 5.1](#)).

Wir empfehlen insbesondere, auf die **Klarheit und Struktur** der Nutzungsbedingungen zu achten. Studien zeigen, dass Nutzer:innen nur wenig Zeit mit dem Lesen der Nutzungsbedingungen verbringen und

die dargebotenen Informationen wenig konzentriert verarbeiten; die Nutzungsbedingungen wirken vielmehr als Appell an das Rechtsbewusstsein der Nutzer:innen^{1,2}. Um die Navigation und das Verständnis der Nutzungsbedingungen zu erleichtern, ist es ratsam, Zeit in die visuelle Gestaltung der Nutzungsbedingungen zu investieren und mit klaren Überschriften oder Aufzählungen zu arbeiten. Es kann auch sinnvoll sein, die Nutzer:innen von Zeit zu Zeit an bestimmte Aspekte der Nutzungsbedingungen zu erinnern oder bei verdächtigem Verhalten über ein Pop-up-Fenster vor möglichen Konsequenzen zu warnen².

Bei der Erstellung und Überarbeitung der Nutzungsbedingungen kann die folgende **Checkliste** als Leitfaden dienen, um die Einhaltung der TCO-Verordnung zu optimieren.



Definieren Sie terroristische Inhalte

Eine zweckmäßige Definition von Terrorismus und terroristischen Inhalten ist wichtig, um Inhalte und Verhaltensweisen daran messen zu können. Diese Definition sollte in den Nutzungsbedingungen dargelegt werden und bei der Bewertung von Inhalten herangezogen werden. Bestehende Definitionen, die in diesem Leitfaden bereits vorgestellt und erörtert wurden (siehe ► [Definition hier](#)), insbesondere die der EU auf der Grundlage der [EU-Richtlinie 2017/541](#), können in dieser Hinsicht eine nützliche Orientierungshilfe bieten.



Legen Sie die Strategie zur Bekämpfung terroristischer Inhalte offen

Die TCO-Verordnung verpflichtet HSPs, die terroristischen Inhalten ausgesetzt sind, in den Nutzungsbedingungen sowohl die Strategie zu erläutern, mit der sie die Verbreitung terroristischer Inhalte zu bekämpfen beabsichtigen, als auch alle eingesetzten automatisierten Mittel (z. B. zur Identifizierung verbotener Inhalte; ► [Kapitel 2](#)). Die TCO-Verordnung verpflichtet HSPs ferner, spezifische Maßnahmen zu ergreifen, sobald sie terroristischen Inhalten ausgesetzt sind (z. B. Systeme zur Meldung schädlicher Inhalte durch Nutzer:innen oder Beschwerdesysteme zum Widerspruch der Entfernung von Inhalten aufzubauen; ► [Kapitel 4](#)) ([TCO-Verordnung, Art. 7.1](#)).



Ziehen Sie Designationslisten heran und erwägen Sie ein klares Verbot anderer Arten schädlicher Inhalte

Verschiedene Arten an Inhalten können für die Nutzer:innen, die Gesellschaft und die Plattform selbst schädlich sein. Daher sollte ein HSP erwägen, weitere zusätzliche Inhalte zu verbieten, die beispielsweise auch in anderen Gesetzen eine Rolle spielen, wie Hassrede oder Aufforderungen zur Gewalt. Auf der Ebene der Akteur:innen können terroristische Gruppierungen von der Nutzung der Plattform ausgeschlossen werden. [Designationslisten](#) (d. h. offizielle, von demokratischen Staaten veröffentlichte Listen terroristischer Gruppen) sind eine gute Quelle für solche Verbote. Darüber hinaus können die zuständigen Behörden die HSPs auf Inhalte aufmerksam machen, die zwar nicht als terroristisch, aber dennoch als schädlich eingestuft werden; die

¹ Obar, J. A., & Oeldorf-Hirsch, A. The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. *Information, Communication & Society*, 23(1), 128–147. <https://doi.org/10.1080/1369118X.2018.1486870>

² Robinson, E. P., & Zhu, Y. (2020). Beyond "I Agree": Users' Understanding of Web Site Terms of Service. *Social Media + Society*, 6(1), 1–13. <https://doi.org/10.1177/2056305119897321>

Bewertung der Inhalte anhand der Nutzungsbedingungen und die eventuelle Behandlung nicht-terroristischer, aber schädlicher Inhalte liegt letztlich in der Verantwortung der HSPs ([TCO-Verordnung, 40](#)).



Beschreiben Sie akzeptierte Nutzungsweisen

Die Nutzungsbedingungen sollten auch in Relation zum Konzept der Plattform beschreiben, welche Nutzungsverhaltensweisen von der HSP nicht nur akzeptiert, sondern auch begrüßt und erwünscht werden. Hierfür gibt es keinen allgemeingültigen Standard – je nach den Funktionalitäten und Werten der Plattform variiert dies stark. Dennoch ist die Beschreibung der akzeptierten Nutzung nicht ausdrücklich erforderlich, um die Verpflichtungen der TCO-Verordnung zu erfüllen.



Informieren Sie darüber, wie verbotene Inhalte gemeldet werden können

Eine Möglichkeit, illegale und gegen die Nutzungsbedingungen verstoßende Inhalte aufzudecken, sind Meldesysteme, durch die Nutzer:innen selbst verdächtige Inhalte an den HSP kommunizieren können. HSPs sollten daher einen Abschnitt in die Nutzungsbedingungen aufnehmen, in dem die Verfahren für die Meldung von Inhalten erläutert werden.



Bestimmen Sie die Konsequenzen einer Verletzung der Nutzungsbedingungen

Um sicherzustellen, dass Verstöße gegen die Nutzungsbedingungen transparent gehandhabt werden und gegenüber der Öffentlichkeit verlässlich zu bleiben, sollten HSPs in den Nutzungsbedingungen klar festlegen, welche Maßnahmen gegen eine:n Nutzer:in oder einen Inhalt wegen Verstößen gegen die Nutzungsbedingungen ergriffen werden. Handelt es sich um eine Entfernungsanordnung durch eine zuständige Behörde im Rahmen der TCO-Verordnung, ist die Handhabung unstrittig: Der Inhalt muss innerhalb einer Stunde entfernt werden. Auf die Entfernungsanordnung kann auch mit einer Sperrung des Inhalts oder einem Geoblocking in der EU reagiert werden.



Veröffentlichen Sie jährliche Transparenzberichte

Bei der Ausarbeitung und Überarbeitung der Nutzungsbedingungen sollten sich die HSPs öffentlich dazu verpflichten, regelmäßig Transparenzberichte zu veröffentlichen. Praktische Tipps und die regulatorischen Anforderungen der TCO für die Erstellung von Transparenzberichten folgen in ► [Kapitel 6](#).

Kapitel 2

Spezifische Maßnahmen zur Identifizierung und Entfernung von (terroristischen) Inhalten



Zusammenfassung: Inhalt und Kernpunkte dieses Kapitels

- Die Fähigkeit von HSPs, Inhalte als terroristisch zu erkennen, ist von grundlegender Bedeutung für die Umsetzung der TCO-Verordnung und darüber hinaus.
- In vielen Fällen sind die zu treffenden Entscheidungen nicht einfach, sie können **sehr kontextabhängig und sensibel** sein, und **Grundrechte wie das Recht auf freie Meinungsäußerung müssen sorgfältig berücksichtigt werden**.
- **Was die TCO-Verordnung betrifft, so müssen die Diensteanbieter die Rechtmäßigkeit der von einer zuständigen Behörde ausgeschriebenen Inhalte nicht beurteilen.** Sobald jedoch eine **Entfernungsanordnung** eingegangen ist, haben sowohl der **HSP als auch der oder die Inhaltsanbieter:in (also der oder die Nutzer:in, die einen Beitrag veröffentlicht hat) das Recht, diese anzufechten**.
- Es ist ratsam, einen Prozess aufzubauen, der bei der Identifizierung von terroristischen Inhalten befolgt wird. Ein solcher Prozess besteht aus mehreren Schritten.
- Bei der inhaltlichen Beurteilung spielen verschiedene praktische Erwägungen eine Rolle, z. B. die Verwendung von Designationslisten oder Symboldatenbanken.
- Darüber hinaus spielen Identifizierungsprozesse eine besonders wichtige Rolle im Sonderfall von **grenzüberschreitenden Entfernungsanordnungen**, wenn ein HSP die Entfernungsanordnung nicht von der zuständigen Behörde erhält, in der er seine Hauptniederlassung oder seine:n gesetzlich:en Vertreterin hat. In solchen Fällen **gelten besondere Verfahren**.

Es ist von grundlegender Bedeutung, dass HSPs in der Lage sind zu beurteilen, ob es sich um illegale oder terroristische Inhalte handelt, um terroristische Inhalte proaktiv aufzuspüren und um Entfernungsanordnungen anzufechten, von denen sie glauben, dass sie fälschlicherweise erlassen wurden. Die korrekte Einstufung von Inhalten als (nicht) illegal oder terroristisch ist auch wichtig, um andernfalls legale und nicht terroristische Inhalte online lassen zu können. Solche Entscheidungen sind oft nicht einfach, und es **muss immer abgewogen werden zwischen dem Schaden, der durch die Inhalte entsteht, und**

dem Schaden, der durch die Entfernung des Inhalts hinsichtlich der Verletzung des Grundrechts auf freie Meinungsäußerung entsteht.

1. Warum ist es notwendig, Identifizierungsprozesse für illegale und schädliche Inhalte einzuführen?

Identifizierungsprozesse umfassen eine Reihe von Schritten, die das Unternehmen oder die Plattform unternimmt, um festzustellen, ob Inhalte gegen die TCO-Verordnung oder Elemente der Nutzungsbedingungen einer Plattform verstoßen. Diese Schritte sollten zu einer Beurteilung führen und eine begründete Schlussfolgerung über die Rechtswidrigkeit von Inhalten ermöglichen.

Solche Abwägungsentscheidungen sind dringend **erforderlich, um (a) proaktive Maßnahmen** gegen terroristische und/oder anderweitig schädliche Inhalte **zu ergreifen und (b) strittige Fälle von Entfernungsanordnungen anzufechten**, die von der zuständigen Behörde auf Grundlage der TCO-Verordnung erlassen wurden (weitere Informationen zum Anfechtungsverfahren folgen in ► [Abschnitt 4 dieses Kapitels](#)).

Proaktive Maßnahmen gegen terroristische und andere schädliche Inhalte werden aus verschiedenen Gründen empfohlen.

1. Durch die Umsetzung solcher Maßnahmen demonstrieren HSPs Zuverlässigkeit und Wohlwollen gegenüber den politischen Entscheidungsträger:innen, den zuständigen Behörden und anderen relevanten Akteur:innen.
2. Proaktive Maßnahmen schaffen Vertrauen bei den Beteiligten, da sie die rechtliche Haftung oder den Rufschaden, der durch eine terroristische Ausnutzung der Plattform entstehen könnte, positiv begrenzen.
3. Unzureichende oder unangemessene Maßnahmen gegen terroristische, extremistische oder anderweitig schädliche Inhalte können dazu führen, dass die Plattform Nutzer:innen anzieht, die genau solche Inhalte verbreiten wollen. Die Folge wäre eine zunehmende Verbreitung verbotener Inhalte, was wiederum zu einem größeren Aufwand an Zeit, Mühe und finanziellen Mitteln auf Seiten der HSP führt, die es schließlich zu bekämpfen gilt.

2. Ein Prozess zur Identifizierung terroristischer Inhalte

1) Definition terroristischer Inhalte

Jede Klassifizierung von Inhalten erfolgt unter Bezugnahme auf eine Definition. Was die TCO-Verordnung betrifft, so greift die Definition terroristischer Inhalte auf [EU-Richtlinie 2017/541](#) zurück, wie in der ► [Einleitung](#) erwähnt. Sie definiert terroristische Inhalte als textliche, visuelle oder auditive Inhalte,

„die jemanden zur Begehung terroristischer Straftaten oder zu einem Beitrag zur Begehung dieser Straftaten anstiften oder dazu bestimmten, jemanden zur Beteiligung an Handlungen einer terroristischen Vereinigung zu bestimmen, terroristische Aktivitäten verherrlichen, unter anderem auch durch die Verbreitung von Materialien, die Bilder von terroristischen Anschlägen zeigen. Unter die Definition sollten auch Materialien fallen, die zum Zweck der Begehung oder des Beitrags zur Begehung terroristischer Straftaten Anleitungen zur Herstellung oder Verwendung

von Sprengstoffen, Schusswaffen oder anderen Waffen oder schädlichen oder gefährlichen Stoffen sowie chemischen, biologischen, radiologischen und nuklearen Stoffen (CBRN-Stoffen) oder zu anderen spezifischen Methoden oder Verfahren, einschließlich der Auswahl von Anschlagszielen, enthalten.“ ([TCO-Verordnung, 11](#))

Die Definition umfasst keine „Materialien, die für Bildungs-, Presse- oder Forschungszwecke oder für künstlerische Zwecke oder zum Zweck der Sensibilisierung gegenüber terroristischen Aktivitäten verbreitet werden“ ([TCO-Verordnung, 12](#)), und Grundrechte wie die Meinungs-, Informations- und Wissenschaftsfreiheit sind stets sorgfältig zu berücksichtigen. „. Ferner sollte die Formulierung radikaler, polemischer oder kontroverser Ansichten zu sensiblen politischen Fragen in der öffentlichen Debatte nicht als terroristischer Inhalt betrachtet werden.“ ([TCO-Verordnung, 12](#))

2) Unterstützung durch den Einsatz von automatisierten Tools

Es kann oft sehr hilfreich sein, automatisierte Tools für die vorläufige Identifizierung potenziell problematischer Inhalte einzusetzen. So können beispielsweise bestimmte [Schlüsselwörter](#) oder [visuelle Elemente](#) wie Logos oder Symbole, die mit extremistischen Weltanschauungen oder terroristischen Organisationen in Verbindung gebracht werden, automatisiert ermittelt werden. Es gibt auch Initiativen zur automatischen plattformübergreifenden Erkennung potenziell terroristischer Inhalte, die auf eine gemeinsame Datenbank zurückgreifen (z. B. die [Terrorist Content Analytics Platform](#) [TCAP] von Tech Against Terrorism oder die vom Global Internet Forum to Counter Terrorism [GIFCT] unterhaltene [Hash-Sharing-Datenbank](#)).

3) Unterstützung durch Meldesysteme

Wenn ein HSP terroristischen Inhalten ausgesetzt ist – formal bedeutet dies, dass die zuständige Behörde des Landes, in dem sich die Hauptniederlassung des HSPs befindet oder in dem der oder die gesetzliche Vertreter:in ansässig ist, mindestens zwei rechtsverbindliche Entfernungsanordnungen erlassen hat und die HSP davon in Kenntnis gesetzt wurde – verlangt die TCO-Verordnung ausdrücklich, dass Maßnahmen ergriffen werden, um die Verbreitung terroristischer Inhalte zu verhindern ([TCO-Verordnung, Art. 5.2](#)). Es werden jedoch auch präventive Maßnahmen empfohlen, um proaktives Verhalten zu zeigen. Eine solche Maßnahme kann ein Meldesystem sein, das es den Nutzer:innen ermöglicht, verdächtige und verbotene Inhalte an den HSP zu melden. Es ist sinnvoll, die Nutzer:innen eine Kategorie angeben zu lassen, die sie den verdächtigen Inhalten zuordnen würden. Terrorismus sollte als eigene Kategorie benannt werden. So können die Mitarbeiter:innen, die die Meldungen bearbeiten, Inhalte, die im Verdacht stehen, terroristisches Gedankengut zu verbreiten, schneller priorisieren und bearbeiten. Diese Vorkategorisierung kann auch die Erstellung von späteren Transparenzberichten erleichtern – mehr dazu in ► [Kapitel 6](#).

4) Zuordnung von und Überprüfung durch menschliche Moderator:innen

Die Kennzeichnung von Inhalten durch automatisierte Tools oder die Meldung durch einzelne Nutzer:innen ist der erste Schritt, um die Aufmerksamkeit auf verdächtige, potenziell gefährliche Inhalte zu lenken. Anschließend ist jedoch in der Regel eine Überprüfung durch menschliche Moderator:innen erforderlich, bis eine endgültige Entscheidung über die zu treffenden Maßnahmen möglich ist. Diese

Moderator:innen sollten (1) mit den für die Plattform geltenden Vorschriften vertraut sein, (2) in der Lage sein, verbotene Inhalte von Inhalten zu unterscheiden, die durch das Grundrecht auf freie Meinungsäußerung abgedeckt sind, und (3) über genaue Kenntnisse der verschiedenen Moderationsmöglichkeiten auf der Plattform verfügen. Es ist wichtig, dass menschliche Moderator:innen ständig über terroristische Online-Strategien geschult werden, aber aus ethischer Sicht ist es nicht weniger wichtig, dass sie Beratung über die psychologischen Auswirkungen des Umgangs mit problematischen Inhalten erhalten können.

5) Entscheidung über den Umgang mit dem entsprechenden Inhalt

Der oben beschriebene Prozess mündet schließlich in einer Entscheidung darüber, wie mit dem Inhalt umgegangen werden soll. Es kann sein, dass nichts unternommen wird und der Inhalt aktiv bleibt, wenn er nach Abwägung und Beurteilung als unbedenklich eingestuft wird. Im anderen Extremfall, wenn es sich um höchst problematische, gefährliche oder anderweitig verbotene Inhalte handelt, wie z. B. Aufrufe zu terroristischen Anschlägen, können Inhalte und Accounts gesperrt werden. Dazwischen gibt es jedoch auch zahlreiche andere Möglichkeiten, mit Inhalten umzugehen: Inhalte, die nicht in den Anwendungsbereich der TCO-Verordnung fallen, erfordern möglicherweise eine differenziertere Behandlung. Einzelheiten und praktische Vorschläge finden Sie im folgenden ► [dritten Kapitel](#) über wirksame Moderationsstrategien.

6) Benachrichtigung der Person, die den Inhalt anbietet

Wenn ein Inhalt gesperrt wird, muss der oder die Inhaltenanbieterin benachrichtigt werden. Hierfür wird ein automatisches Benachrichtigungs- und Beschwerdesystem empfohlen. Generell sollte dazu ein für den HSP geeignetes Verfahren entwickelt und eingerichtet werden. Einzelheiten und Vorschläge, wie dies im Einklang mit der TCO-Verordnung geschehen kann, finden Sie im ► [fünften Kapitel](#).

3. Praktische Tipps und Ratschläge: Was hilft bei der Beurteilung, ob ein Inhalt illegal ist?

Was die **TCO-Verordnung** betrifft, so **müssen HSPs die Rechtmäßigkeit von Inhalten nicht beurteilen**, da dies in der Verantwortung der zuständigen Behörden liegt, bevor sie eine Entfernungsanordnung erteilen. Allerdings sind **HSPs verpflichtet, terroristische Inhalte auf ihren Plattformen proaktiv zu identifizieren, sobald sie terroristischen Inhalten ausgesetzt sind**. Es ist oft schwierig zu beurteilen, ob ein Inhalt tatsächlich die rechtliche Grenze überschreitet und daher verboten ist. Darüber hinaus sollte die psychische Belastung, die durch die Sichtung problematischer Inhalte entsteht, nicht vernachlässigt werden. Mitarbeiter:innen, die Inhalte moderieren, sollten regelmäßig die Möglichkeit haben, ihre Arbeit zu reflektieren und bei Bedarf psychologische Unterstützung zu erhalten.

Um die Rechtswidrigkeit von Inhalten zu beurteilen, finden Sie im Folgenden einige Hinweise und praktische Tipps. Werfen wir zunächst einen Blick auf die relevanten Teile der TCO-Verordnung zur Bewertung von Inhalten:

In Absatz 11 heißt es u. a.:

„Bei der Beurteilung, ob es sich bei Materialien um terroristische Inhalte im Sinne dieser Verordnung handelt, sollten die zuständigen Behörden und die Hostingdiensteanbieter Faktoren wie Art und Wortlaut der Aussagen, den Kontext, in dem die Aussagen getroffen wurden, und ihr Gefährdungspotenzial und somit ihr Potenzial zur Beeinträchtigung der Sicherheit von Personen berücksichtigen.“ ([TCO-Verordnung, 11](#))

Außerdem müssen die Grundrechte immer gegeneinander abgewogen werden:

„Bei der Feststellung, ob es sich bei den von einem Inhaltenanbieter bereitgestellten Materialien um „terroristische Inhalte“ im Sinne dieser Verordnung handelt, sollte insbesondere dem Recht auf Meinungs- und Informationsfreiheit, einschließlich der Medienfreiheit und des Medienpluralismus, und der Freiheit von Kunst und Wissenschaft Rechnung getragen werden. Insbesondere in Fällen, in denen der Inhaltenanbieter eine redaktionelle Verantwortung trägt, sind Entscheidungen über die Entfernung verbreiteter Materialien unter Berücksichtigung der in einschlägigen Presse- und Medienvorschriften festgelegten journalistischen Standards, die im Einklang mit dem Unionsrecht einschließlich der Charta stehen, zu treffen.“ ([TCO-Verordnung, 12](#))

Wenn ein HSP eine Entfernungsanordnung erhält, wurde der Inhalt von der zuständigen Behörde bereits als terroristisch eingestuft. In zwei Szenarien ist es für die HSP nützlich, in der Lage zu sein, um Inhalte als terroristisch oder nicht-terroristisch einstufen zu können:

1. Wenn ein HSP noch keine offizielle Entfernungsanforderung erhalten hat, aber **proaktiv handeln** und/oder die Einhaltung seiner eigenen Nutzungsbedingungen in Bezug auf verdächtige Inhalte durchsetzen möchte.
2. Wenn eine HSP eine Entfernungsanordnung erhält, aber **Zweifel** an der Einstufung des Inhalts als terroristisch durch die zuständige Behörde hat und die Anordnung überprüfen lassen möchte (als ersten Schritt zu einem Rechtsbehelf).

Nachfolgend finden Sie verschiedene praktische Tipps, die Ihnen bei der Einstufung von Inhalten als terroristisch oder nicht-terroristisch helfen können.



Ziehen Sie Designationslisten heran

Nationale und internationale [Designationslisten](#), die terroristische Organisationen benennen, bieten einen guten Rahmen und Bezugspunkt für die Klassifizierung von Inhalten. Die Zuhilfenahme von Designationslisten als Grundlage für ein Verbot oder eine Sperrung, auf die in den Nutzungsbedingungen (► [Kapitel 1](#)) verwiesen werden sollte, gibt den Sanktionen einer Plattform den nötigen rechtlichen Rückhalt. Absatz 11 der [TCO-Verordnung](#) schlägt ausdrücklich vor, dass die Liste der Europäischen Union bei der Bewertung von Inhalten verwendet werden kann.



Nutzen Sie Stichwort-, Symbol- und Logodatenbanken

Die Personen, die die Inhalte manuell prüfen, sollten nicht nur die Definition terroristischer Inhalte parat haben, sondern auch mit den von terroristischen Organisationen typischerweise verwendeten Schlüsselwörtern und Phrasen vertraut sein und diese Kenntnisse pflegen. Je intensiver eine Person, die den Inhalt beurteilt, mit einem terroristischen Phänomenbereich (z. B. rechts, links, islamistisch) vertraut ist, desto leichter lassen sich Verschleierungstaktiken wie das so genannte "Dog Whistling" erkennen, d. h. die Verwendung scheinbar harmloser Wörter, die innerhalb der Szene ideologische Bedeutungen haben³. Eine Datenbank mit Logos und Symbolen, d. h. visuellen Elementen, die auf einen terroristischen Hintergrund hinweisen, ist ebenfalls unverzichtbar für eine genaue und zügige Bewertung der Inhalte.



Beziehen Sie Kontextfaktoren ein

Bei der Moderation sollte der Kontext berücksichtigt werden, in dem die Inhalte wahrscheinlich veröffentlicht wurden. Zu den relevanten Kontextfaktoren gehören unter anderem (a) politische Rahmenbedingungen, (b) aktuelle Ereignisse, einschließlich jüngsten Nachrichtengeschehens, und (c) kulturelle Umstände, die die Ansichten zu bestimmten Themen prägen können. Dies ist oft schwer zu beurteilen – vor allem, wenn die Nutzer:innen anonym sind und die von ihnen geposteten Inhalte nur wenige oder gar keine textlichen Hinweise auf ihre Identität enthalten. In einigen Fällen jedoch, wenn in den Inhalten auf externe Faktoren Bezug genommen wird, können sich Kontextüberlegungen als überaus hilfreich erweisen.

Wenn Sie es mit **Inhalten** zu tun haben, die **nicht terroristisch, sondern auf andere Weise schädlich sind** (z. B. verschiedene Formen von Hassrede), können Sie auch die folgenden Punkte berücksichtigen.



Wägen Sie das Ausmaß des durch den Inhalt verursachten möglichen Schadens ab

Terroristische, extremistische und andere hassvolle Inhalte, insbesondere wenn sie zur Begehung terroristischer Straftaten oder Gewalt auffordern, können erheblichen Schaden verursachen. Bei der Bewertung von Inhalten kann es sinnvoll sein, das Ausmaß zu berücksichtigen, in dem die Inhalte einen solchen Schaden verursachen können. Je größer der Schaden ist, der entstehen kann, desto schneller und gezielter müssen Maßnahmen ergriffen werden. Nachteilige psychologische Auswirkungen auf die von den schädlichen Inhalten Betroffenen sollten als eine Form des Schadens betrachtet werden.



Berücksichtigen Sie die möglichen Auswirkungen der Entfernung des Inhalts

Die TCO-Verordnung fordert eine sensible Abwägung der in der Charta verankerten Grundrechte (z. B. Meinungs- und Informationsfreiheit), wenn es um die Entfernung von Inhalten geht. Wenn die Entfernung nicht von einer zuständigen Behörde angeordnet wurde, gibt es andere Möglichkeiten, wie mit schädlichen Inhalten umgegangen werden kann – Beispiele dafür finden Sie in

► [Kapitel 3](#).

³ Åkerlund, M. (2022). Dog whistling far-right code words: the case of 'culture enricher' on the Swedish web. *Information, Communication & Society*, 25(12), 1808-1825. <https://doi.org/10.1080/1369118X.2021.1889639>

4. Was soll ich tun, wenn ich es anders sehe? Eine erhaltene Entfernungsanordnung anfechten

Was ist zu tun, wenn die Beurteilung des HSP und der zuständigen Behörde einander widersprechen?

Sowohl die HSPs als auch die Inhaltsanbieter haben das Recht, gegen Entfernungsanordnungen gemäß [Artikel 9](#) der TCO-Verordnung vorzugehen. Dieses Recht ist ein wichtiges Kontrollinstrument zur Wahrung der Grundrechte.

Die Anfechtung von Entfernungsanordnungen erfolgt vor den Gerichten des EU-Mitgliedstaates, dessen zuständige Behörde die Entfernung angeordnet hat. **Die HSPs sind verpflichtet, alle Inhalte, die entfernt wurden (entweder aufgrund einer Entfernungsanordnung oder anderer Maßnahmen), sowie alle mit den Inhalten verbundenen Daten (z. B. Zeitpunkt der Veröffentlichung, Accountinformationen) unter sicheren Bedingungen und für einen Zeitraum von sechs Monaten aufzubewahren.** Dies dient der Untersuchung und Verhinderung terroristischer Straftaten oder Bedrohungen und gewährleistet, dass genügend Zeit zur Verfügung steht, um die Entfernung von Inhalten rechtlich anzufechten und sie gegebenenfalls wiederherzustellen ([TCO-Verordnung, 27 & 28](#)).

Sonderfall: Grenzüberschreitende Entfernungsanordnungen ([TCO-Verordnung, Art. 4](#))

Erhält ein HSP eine Entfernungsanordnung von einer zuständigen Behörde in einem anderen EU-Mitgliedstaat als ihrer ‚Heimatbehörde‘ (d. h. der zuständigen Behörde des Mitgliedstaats, in dem der HSP seine Hauptniederlassung oder seine:n gesetzliche:n Vertreter:in hat; Einzelheiten zu gesetzlichen Vertretern folgen in ► [Kapitel 4](#)), **gilt ein besonderes Verfahren.**

Beim Erlass der Entfernungsanordnung muss die zuständige Behörde auch eine Kopie dieser Anordnung an die Heimatbehörde senden. Diese kann die Entfernungsanordnung dann innerhalb von 72 Stunden überprüfen. Wird festgestellt, dass die Entfernungsanordnung gegen die in der Charta verankerten Grundrechte und -freiheiten verstößt, kann sie eine begründete Entscheidung erlassen, ob es sich um einen Verstoß handelt.

Der HSP muss die Inhalte nach Erhalt der Entfernungsanordnung wie gehabt entfernen und sichern (also so, wie auch im Falle einer Entfernungsanordnung durch die Heimatbehörde). Der HSP (und der oder die Inthalteanbieter:in) können innerhalb von 48 Stunden einen Antrag auf Überprüfung bei der Heimatbehörde stellen. Diese überprüft die Entfernungsanordnung schließlich, nachdem sie die zuständige Behörde, die die Entfernung ursprünglich angeordnet hat, über die Überprüfung informiert hat.

Nachdem die überprüfende Behörde – also die Heimatbehörde – eine begründete Entscheidung erlassen hat, werden die betroffenen Akteur:innen (d. h. die ursprüngliche Behörde, der HSP, der oder die Inhaltsanbieter:in und gegebenenfalls Europol) benachrichtigt, und wenn ein Verstoß festgestellt wurde, stellt der HSP den Inhalt unverzüglich wieder her.

Kapitel 3

Etablierung wirksamer Moderationsmechanismen für terroristische Online-Inhalte



Zusammenfassung: Inhalt und Kernpunkte dieses Kapitels

- Bei der Inhaltsmoderation werden die **Inhalte der Nutzer:innen daraufhin überprüft, ob gesetzliche** (z. B. TCO-Verordnung, DSA) **und plattformspezifische Regelungen** (z. B. Nutzungsbedingungen) **eingehalten oder verletzt werden**.
- **Wenn gegen eine Regel verstoßen wurde, wird der Inhalt ‚moderiert‘**. Das heißt, es werden Maßnahmen ergriffen, um die Reichweite des Inhalts zu begrenzen.
- Wenn eine zuständige Behörde auf der Grundlage der TCO-Verordnung die **Entfernung von Inhalten anordnet, beinhaltet die Inhaltsmoderation immer die Entfernung** der betreffenden terroristischen Inhalte. Der HSP und der oder die Inhaltenanbieter:in können die Entfernungsanordnung anfechten, wenn sie damit nicht einverstanden sind.
- Vor, während oder kurz nach der Durchführung der Moderationsmaßnahmen durch den HSP sowie bei einer späteren Überprüfung sind verschiedene Punkte zu beachten. Diese umfassen die Benachrichtigung der Nutzer:innen, deren Inhalt moderiert wurde, und die Möglichkeit einer Anfechtung der Entscheidung.
- Wenn Plattformen unabhängig von der TCO-Verordnung **proaktiv gegen andere potenziell schädliche Formen von Inhalten** wie Hassreden oder Beleidigungen vorgehen, können auch andere **alternative Moderationsansätze** in Betracht gezogen werden.

1. Was ist Inhaltsmoderation und warum ist sie in manchen Fällen notwendig?

Bei der Inhaltsmoderation geht es um die **Überprüfung von nutzergenerierten Online-Inhalten**, um die **Angemessenheit** der Inhalte auf der Grundlage der Nutzungsbedingungen und rechtlichen Rahmenbedingungen (z. B. TCO-Verordnung, DSA) **beurteilen zu können**⁴. Diese **werden durch die Moderation von Inhalten durchgesetzt**, sodass Maßnahmen gegen verbotene und/oder problematische Inhalte ergriffen werden. HSPs sind aufgefordert, die spezifischen Maßnahmen, die sie zur Erkennung und Entfernung terroristischer Inhalte ergreifen, **transparent zu machen**, einschließlich proaktiver und reaktiver Verfahren zur Inhaltsmoderation und aller verwendeten automatisierten Tools.

⁴ Roberts, S. T. (2017). Content Moderation. In L. Schintler & C. McNeely (Hrsg.): *Encyclopedia of Big Data*. Springer, Cham. https://doi.org/10.1007/978-3-319-32001-4_44-1

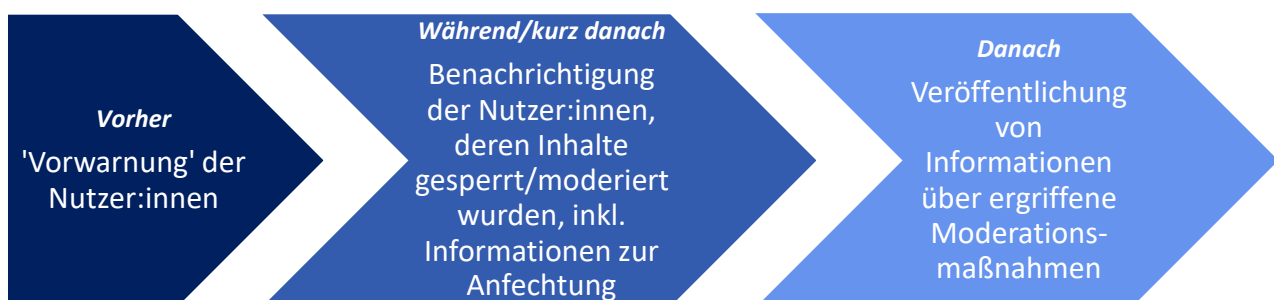
Die Moderation von Inhalten ist ein sehr wichtiges, aber auch sehr kompliziertes und **sensibles** Verfahren. Die Bereitstellung der entsprechenden technischen und fachlichen Ressourcen kann für kleinere Unternehmen eine erhebliche finanzielle Belastung darstellen. Außerdem können terroristische Inhalte in allen Sprachen produziert werden, und es ist äußerst ressourcenintensiv, sicherzustellen, dass die Moderator:innen in der Lage sind, Inhalte in all diesen Sprachen zu begutachten.

Die in der UN-Menschenrechtserklärung verankerten Grundrechte, insbesondere das Recht auf freie Meinungsäußerung, müssen immer gegen den Schaden abgewogen werden, der durch den betreffenden Inhalt verursacht wird. Zudem haben HSPs auch eine gewisse soziale Verantwortung, schädliche Inhalte auf ihrer Plattform zu minimieren.

Eine verständliche und transparente Inhaltsmoderation trägt dazu bei, Nutzer:innen und Stakeholder vor den Auswirkungen schädlicher Inhalte zu schützen und Vertrauen zu schaffen. Aus der Sicht der HSPs kann Inhaltsmoderation die Haftungsbeschränkung, die Einhaltung geltender Gesetze und den Schutz vor Rufschädigung durch den Missbrauch der Plattform unterstützen.

Inhaltsmoderation bedeutet nicht zwangsläufig die Entfernung von Inhalten. Während die Löschung von Inhalten aufgrund rechtlicher Anforderungen zwingend sein kann – wie dies bei Entfernungsanordnungen auf der Grundlage der TCO-Verordnung der Fall ist – gibt es andere Möglichkeiten, mit schädlichen Inhalten umzugehen. Je nachdem, wie problematisch und schwerwiegend die Inhalte sind und welchen Schaden sie anrichten können, können alternative Optionen in Betracht gezogen werden. Beispiele und Vorschläge für alternative Moderationsstrategien finden Sie in ► [Abschnitt 3 dieses Kapitels](#).

Moderationsstile variieren von Plattform zu Plattform, abhängig von der Funktionalität, den angebotenen Dienstleistungen, den Werten der Plattform sowie der Risikotoleranz⁵. Es ist wichtig, bei der Moderation so transparent wie möglich vorzugehen. Dazu gehören verschiedene Faktoren, die vor, während und nach der Moderation berücksichtigt werden müssen, um sicherzustellen, dass die Nutzer:innen wissen, welche Maßnahmen zur Moderation ihrer Inhalte ergriffen werden können.



⁵ Roberts, S. T. (2017). Content Moderation. In L. Schintler & C. McNeely (Hrsg.): *Encyclopedia of Big Data*. Springer, Cham. https://doi.org/10.1007/978-3-319-32001-4_44-1

1. **Vorher:** ‚Vorwarnung‘ der Nutzer:innen

Informieren Sie die Nutzer:innen frühzeitig darüber, welche Maßnahmen gegen Inhalte ergriffen werden können, wenn ein Verhalten oder ein Inhalt durch die Nutzungsbedingungen oder durch das Gesetz verboten ist. Dies bedeutet: Nehmen Sie Informationen über Ihre Moderationsstrategien in die verbindliche Vereinbarung mit den Nutzer:innen auf, also in die Nutzungsbedingungen (► [Kapitel 1](#)). Dies trägt dazu bei, dass Sie bereits vor oder bei der Aufnahme der Beziehung zu den Nutzer:innen Vertrauen aufbauen und verbindlich und unmissverständlich zusichern, dass problematische und illegale Inhalte auf der Plattform nicht geduldet werden und dass Sie als HSP die Nutzer:innen vor solchen Inhalten schützen wollen.

2. **Während (bzw. kurz nach) der Maßnahme:** Benachrichtigung der Nutzer:innen, deren Inhalte gesperrt oder moderiert wurden, inkl. Informationen zu Anfechtungsmöglichkeiten

[Artikel 11 der TCO-Verordnung](#) verpflichtet HSPs erstens, die Nutzer:innen, die einen terroristischen Inhalt bereitstellen (d. h. verfasst und/oder hochgeladen haben), darüber zu informieren, dass der Inhalt auf der Plattform gesperrt wurde, und zweitens, die Nutzer:innen auf deren Wunsch über den Hintergrund oder die Anordnung der Sperrung zu informieren. Die Mitteilung muss dem oder der Inhaltsanbieter:in vorübergehend für einen Zeitraum von höchstens sechs Wochen vorenthalten werden, wenn die zuständige Behörde der Auffassung ist, dass die Mitteilung der Entfernung mit einer besonderen Gefahr verbunden ist. Wenn die Nichtbekanntgabe dieser Information weiterhin wichtig und angemessen ist, kann die zuständige Behörde die Frist um weitere sechs Wochen verlängern ([TCO-Verordnung, Art. 11.3](#)). Die TCO-Verordnung ([Art. 10](#)) sieht spezifische Beschwerdemechanismen für den Umgang mit solchen Situationen vor. Es empfiehlt sich, ein standardisiertes Verfahren einzurichten, mit dem die Inhaltsanbieter:innen über die Löschung benachrichtigt werden und die Möglichkeit erhalten, dagegen Beschwerde einzulegen. Dieser Benachrichtigungs- und Beschwerde-mechanismus sollte auch in Fällen eingesetzt werden, die nicht unter die TCO-Verordnung fallen, sondern durch (pro-)aktive Maßnahmen seitens der HSP-Inhaltsmoderator:innen zustande gekommen sind.

3. **Danach:** Regelmäßige öffentliche Bekanntgabe von Informationen zu HSP-weiten Moderationsmaßnahmen

Transparenz in Bezug auf Entscheidungen und Ergebnisse der Inhaltsmoderation ist wichtig, um Vertrauen und Verantwortlichkeit zwischen dem HSP und den Nutzer:innen zu schaffen, und wird zunehmend durch verschiedene Arten von Online-Vorschriften vorgeschrieben. In Transparenzberichten werden Informationen über die Moderationsentscheidungen einer Plattform erfasst, die nicht nur die Anzahl und die Art der festgestellten Verstöße betreffen, sondern auch die genaue Art und Weise, wie mit diesen Verstößen umgegangen wurde. (Weitere Einzelheiten zu Transparenzberichten und speziellen TCO-Transparenzanforderungen finden Sie in ► [Kapitel 6](#)).

2. Praktische Tipps und Ratschläge: Welche Verfahren der Inhaltsmoderation kommen in Frage?

Es ist wichtig, dass HSPs über ein klares **Verfahren zur Inhaltsmoderation** verfügen, das an die spezifischen Unternehmensdienste und -bedürfnisse **angepasst** werden kann. Von entscheidender Bedeutung ist es, zunächst verbotene Inhalte zu identifizieren und ihre Rechtswidrigkeit beurteilen zu können, wie in ► [Kapitel 2](#) näher erläutert. Zur Erinnerung: Dies sind die wichtigsten Schritte:

1. Definition terroristischer Inhalte
2. Unterstützung durch den Einsatz von automatisierten Tools
3. Unterstützung durch Meldesysteme
4. Zuordnung von und Überprüfung durch menschliche Moderator:innen
5. **Entscheidung über den Umgang mit dem entsprechenden Inhalt (d.h. Entscheidung über die Moderation des Inhalts)**
6. Benachrichtigung der Person, die den Inhalt anbietet

In diesem Abschnitt befassen wir uns mit *Schritt 5*. In ► [Kapitel 2](#) haben wir diesen Schritt ‚Entscheidung über den Umgang mit dem Inhalt‘ genannt. Wenn ein HSP von einer zuständigen Behörde eine Entfernungsanordnung erhalten hat, muss der Inhalt entfernt werden und es kann gegen die Anordnung Widerspruch eingelegt werden. HSPs können sich auch dazu entscheiden, terroristische oder verbotene Inhalte proaktiv zu identifizieren und zu entfernen (wenn keine Entfernungsanordnung ergangen ist).

In diesem Leitfaden werden fünf verschiedene Arten der Moderation unterschieden: prä-, post-, reaktiv, verteilt und automatisiert. Kurze Erklärungen sowie ihre Vor- und Nachteile finden Sie in der Tabelle.

Art der Moderation	Erläuterung
Prä-Moderation	Die Moderator:innen prüfen den Inhalt vor der Veröffentlichung. Vorteile: Hoher Grad an Sicherheit und inhaltlicher Übereinstimmung mit gesetzlichen Standards und plattformspezifischen Vorschriften Nachteile: Hoher Aufwand, Personal- und (eventuelle) finanzielle Kosten
Post-Moderation	Die Moderator:innen prüfen den Inhalt unmittelbar nach der Veröffentlichung. Vorteile: Schnelle Interaktionen der Nutzer:innen mit dem Inhalt möglich (wegen sofortiger Veröffentlichung) Nachteile: Erheblicher Zeit-, Personal- (und eventuell finanzieller) Aufwand; im Falle verbotener/schädlicher Inhalte sind die Nutzer:innen diesen Inhalten ausgesetzt
Reaktive Moderation	Die Moderator:innen prüfen den Inhalt, nachdem ein:e Nutzer:in ihn gemeldet hat.

	Vorteile: Weniger ressourcenintensiver HSP-Aufwand; Vertrauensbildung bei den Nutzer:innen (durch die Möglichkeit der Meldung) Nachteile: Verantwortung der Nutzer:innen; im Falle von verbotenen/schädlichen Inhalten sind die Nutzer:innen den Inhalten ausgesetzt; es kann zu Fehlalarmen kommen, die zusätzlichen Aufwand für die HSP erfordern
Verteilte Moderation	Die Community fungiert als Moderator:innen, z. B. durch Up- und Down-Vote-Mechanismen, der die Vertrauenswürdigkeit des Inhalts misst und dazu dient, die öffentliche Reichweite des Inhalts zu bestimmen (d. h. Inhalte mit vielen Up-Votes werden hochgestuft und erhalten eine höhere Reichweite). Vorteile: Geringerer Ressourcenaufwand; Förderung des Engagements der Nutzer:innen; Selbstregulierung Nachteile: Verantwortung der Nutzer:innen; bei verbotenen/schädlichen Inhalten sind die Nutzer:innen den Inhalten ausgesetzt; Anfälligkeit für koordiniertes manipulatives Verhalten
Automatisierte Moderation	Modelle, die auf künstlicher Intelligenz basieren (z. B. Filter, Algorithmen), fungieren als Moderator:innen. Vorteile: Weniger ressourcenintensiv, wenn es einmal eingerichtet ist; frühzeitige, schnelle, hoch skalierbare Erkennung von potenziell schädlichen Inhalten Nachteile: Fehleranfälligkeit, insbesondere im Hinblick auf fehlerhaftes Löschen von Inhalten (problematisch im Kontext der Meinungsfreiheit, daher menschliche Beurteilung wichtig); kontinuierliche Pflege und Anpassung an neue Entwicklungen notwendig

(Basierend auf Grimes-Viort, 2010)⁶

Es wird empfohlen, mehrere Ansätze zur Moderation von Inhalten zu kombinieren. Die reaktive Moderation kann etwa leicht mit der Prä- oder Post-Moderation kombiniert werden. Oft sind solche **Kombinationen nützlich und in einigen Fällen sogar notwendig**. Automatisierte Moderationsentscheidungen müssen immer überprüft oder zumindest von Menschen nachgeprüft werden, um systematische Verstöße gegen die Grundrechte der Nutzer:innen und Risiken für die Meinungsfreiheit zu vermeiden.

Seien Sie sich bewusst, dass extremistische und terroristische Akteur:innen **Taktiken** anwenden können, **um bekannte Methoden der Inhaltsmoderation zu vermeiden**, unter dem Radar zu operieren und so die Moderation zu umgehen, insbesondere automatische Mechanismen zur Inhaltsmoderation. Zu beliebten Taktiken gehören die *Verkürzung von URLs*, um Filter oder Webseitensperrungen zu umgehen, das *Spiegeln* von Konten und Inhalten, bei dem identische Inhalte/Accounts mehrfach gepostet oder

⁶ Grimes-Viort, B. (2010, 7. Dezember). 6 types of content moderation you need to know about. *Social Media Today*. <https://www.socialmediatoday.com/content/6-types-content-moderation-you-need-know-about>

erstellt werden, um die Moderator:innen zu überfordern und im Falle einer Löschung Backups zur Verfügung zu haben, oder die bewusste *Falschschreibung* eines Worts, um automatische Filter zu umgehen. Verschiedene Umgehungstechniken machen deutlich, wie wichtig menschliche Moderation ist.

Ihre Beteiligung an diesem Leitfaden oder Ihre (zertifizierte) Teilnahme an dem Online-Kurs, der ebenfalls im Rahmen des TATE-Projekts angeboten wird, zeigen, dass Sie an diesen Trends interessiert sind. Weitere Beispiele für die Umgehung der Inhaltsmoderation sowie machbare und wirksame Antworten finden Sie [hier](#) auf der Knowledge Sharing Platform von Tech Against Terrorism.

3. Alternative Moderationsansätze

Moderation muss nicht immer die Löschung von Inhalten bedeuten. Alternative Ansätze, wie sie im Folgenden vorgeschlagen werden, können für HSPs interessant sein, die Inhalte über die Anforderungen der TCO-Verordnung hinaus (pro-)aktiv moderieren wollen. Es ist wichtig zu betonen, dass solche **alternativen Moderationsansätze nicht in den Anwendungsbereich der TCO-Verordnung fallen und nur dann verwendet werden können, wenn Plattformen keine Entfernungsanordnung erhalten haben, sondern nicht-terroristische, anderweitig schädliche Inhalte proaktiv moderieren wollen**. Wenn Sie eine Entfernungsanordnung erhalten, ist das Verfahren klar: Sie müssen den Inhalt entfernen, und alternative Moderationsansätze kommen nicht in Frage.



SIE WOLLEN MEHR FÜR DIE SICHERHEIT AUF IHRER PLATTFORM TUN?

Inhalt ausblenden

HSPs können Inhalte teilweise oder ganz ausblenden und so eine Sperrung vermeiden, wenn sie finden, dass die Nutzer:innen den Inhalt zwar verwerflich empfinden, er aber dennoch legal und auf der Plattform zulässig ist. Das Ausblenden von Inhalten vor Personen aus einer schutzbedürftigen Gruppe oder Personen, die sich in einem Land befinden, in dem der Inhalt illegal ist (während er in anderen Ländern erlaubt ist), ist möglich. Um Inhalte zu verbergen, können verschiedene technische Funktionen eingesetzt werden, z. B. Anmelde- oder Paywall-Filter, ein sicherer (Such-)Modus zur Anzeige altersgerechter Inhalte und Geo- oder Zeitsperren.

Entkopplung von Inhalt und Belohnungsmechanismen (‘Disengagement’)

Disengagement entzieht bestimmten Inhalten oder Nutzer:innen Engagement-Metriken, schreckt von Aktivitäten im Zusammenhang mit dem Beitrag ab und kann dazu führen, dass es sich generell nicht lohnt, Inhalte zu posten. Der Inhalt und das Nutzer:innenkonto verbleiben jedoch auf der Plattform. Disengagement schränkt den Bekanntheitsgrad von Beiträgen oder Konten auf der Plattform ein. Zu den typischen Disengagement-Taktiken gehören die Deaktivierung von Plattformfunktionen, wie z. B. im Falle vieler sozialer Netzwerke die Möglichkeit, Beiträge zu ‚ liken‘, zu kommentieren oder zu teilen, dass der Beitrag nur noch gelesen werden kann, die Demonetisierung (d. h., dass Konten die Möglichkeit genommen wird, mit ihren Inhalten Geld zu verdienen) oder die Deverifizierung (d. h., dass jegliche Zertifizierung der Identität des Kontos entfernt wird). Solche Sanktionen können eine Änderung der Behandlung des Inhalts oder des Kontos durch den Algorithmus der Plattform nach sich ziehen: Eine

Herabstufung des Inhalts bedeutet, dass es schwieriger ist, ihn über die Mechanismen der Plattform (in der Regel Empfehlungsalgorithmen) zu verbreiten und zu fördern.

Versehen des Inhalts mit pädagogischen Hinweisen

Das Ziel von pädagogischen oder kommunikationsbasierten Taktiken ist es, den Nutzer:innen zusätzliche Informationen anzubieten, damit sie letztendlich selbst entscheiden können, ob sie den Inhalt sehen wollen oder nicht. Dabei entscheidet der HSP, welche Inhalte mit solchen Hinweisen versehen werden, was diese Hinweise beinhalten, vor welcher Art von Schäden die Nutzer:innen gewarnt werden und wie viele zusätzliche Informationen angeboten werden. Eine solche Taktik ist von (vormals) Twitter bekannt: Dort wurden die Nutzer:innen darauf hingewiesen, dass ein Beitrag möglicherweise schädliche Inhalte enthält, wie z. B. Fehlinformationen oder Verschwörungserzählungen. Um diese Inhalte einzusehen, war dies aktiv zu bestätigen. Insbesondere bei politisch-ideologischen Inhalten, die eine Radikalisierung begünstigen könnten, können Counter-Narrative und Links zu Aufklärungs- und Präventionsinformationen, die für die möglichen Auswirkungen solcher Inhalte sensibilisieren, in Erwägung gezogen werden.

Übertragung der Verantwortung an die Nutzer:innen („Community Empowerment“)

Die Prämisse von Moderationsmechanismen, die auf der Community Empowerment beruht, besteht darin, den Nutzer:innen selbst die Möglichkeit zu geben, einen digitalen Raum zu schaffen, wie sie ihn sich vorstellen. Solche Strategien können für Plattformen von besonderem Interesse sein, bei denen der Gedanke der Community eine wichtige Rolle spielt oder deren Moderationspraktiken bereits bis zu einem gewissen Grad von der Unterstützung der Nutzer:innen abhängig sind. Diese Moderationsansätze folgen dem Typus der verteilten Moderation. Dazu gehören neben der bereits erwähnten Up- und Down-Voting-Funktionalität auch das individuelle Sperren oder Stummschalten bestimmter Accounts, das eine Vielzahl von Plattformen bereits anbietet, oder der Einsatz von Admins oder Moderator:innen aus der Community selbst. Eng damit verbunden ist das Konzept der *Trusted Flaggers* (dt: Vertrauenswürdige Hinweisgeber:innen), das im [Digital Services Act \(Artikel 22\)](#) eine wichtige Rolle spielt. Das Konzept bezieht sich auf Nutzer:innen, die besonders vertrauenswürdig und kompetent sind, um die Rechtswidrigkeit von Inhalten zu beurteilen und diese (objektiv und schnell) zu melden, und die unabhängig von der spezifischen Online-Plattform kollektive (gemeinwohlorientierte) Interessen vertreten. Derart gemeldete Inhalte sollen auf der HSP-Seite vorrangig und schnell bearbeitet werden.

Diese alternativen Moderationsansätze können auch dann relevant sein, wenn die Plattformen durch die TCO-Verordnung nicht zum Handeln gezwungen sind. Unabhängig von der Ausgestaltung sieht die TCO-Verordnung einen proaktiven Ansatz vor: Stößt ein HSP im Zuge (pro-)aktiver, eigener Moderationsmaßnahmen auf Inhalte, die eine unmittelbare Bedrohung des Lebens oder eine terroristische Inhalte zum Gegenstand haben, müssen diese gelöscht und die zuständige Behörde des betroffenen EU-Mitgliedstaates unverzüglich informiert werden ([TCO-Verordnung, Art. 14.5](#)).

Nähere Einzelheiten zu den (technischen) Methoden, die für alternative Moderationsansätze in Frage kommen und erforderlich sind, sowie zu ihren Vor- und Nachteilen und Fallstudien finden Sie [hier](#) bei Tech Against Terrorism.

Kapitel 4

Einrichtung von Kontaktstellen und gesetzlichen Vertreter:innen



Zusammenfassung: Inhalt und Kernpunkte dieses Kapitels

- In der TCO-Verordnung wird zwischen Kontaktstellen und gesetzlichen Vertreter:innen unterschieden.
- **Jeder HSP muss eine Kontaktstelle einrichten**, die für die Entgegennahme von **Entfernungsanordnungen** und deren rasche Bearbeitung **zuständig** ist.
- **Wenn der HSP nicht in der EU ansässig ist, muss auch ein:e gesetzliche:r Vertreter:in ernannt werden.** Diese Person ist für die Entgegennahme, Einhaltung und Durchsetzung der TCO-Verordnung verantwortlich. Der oder die gesetzliche Vertreter:in kann, muss aber nicht, gleichzeitig als Kontaktstelle fungieren.
- Jeder HSP, unabhängig davon, ob er terroristischen Inhalten ausgesetzt ist oder nicht, muss gemäß der TCO-Verordnung eine Kontaktstelle und gegebenenfalls eine:n gesetzliche:n Vertreter:in benennen.

Die TCO-Verordnung sieht vor, dass *alle* HSPs, die von dieser Verordnung betroffen sind (d.h. per Definition in den Anwendungsbereich der Verordnung fallen; ► [siehe den Abschnitt über betroffene Plattformen in der Einleitung](#)), verpflichtet sind, eine Kontaktstelle und/oder eine:n gesetzliche:n Vertreter:in zu benennen.

1. Was sind Kontaktstellen und gesetzliche Vertreter:innen?

Kontaktstelle (TCO-Verordnung, 42 & Art. 15)

- **Zweck:** Die HSP-Kontaktstelle erleichtert die sofortige Bearbeitung von Entfernungsanordnungen. Die Kontaktstelle dient daher ausschließlich operativen Zwecken.
- **Logistik:** Die Kontaktstelle sollte in der Lage sein, Entfernungsanordnungen elektronisch zu empfangen und zu übermitteln, unabhängig davon, ob sie intern oder extern angesiedelt ist.
- **Erforderliche Ressourcen:** Die Kontaktstelle muss über ausreichende technische Ressourcen und Zugangsmöglichkeiten verfügen und personell so ausgestattet sein, dass sie Entfernungsanordnungen ohne Verzögerung bearbeiten kann. Da terroristische Inhalte innerhalb einer Stunde nach Erhalt einer Entfernungsanordnung entfernt werden müssen, bedeutet dies, dass die Kontaktstelle rund um die Uhr erreichbar sein muss.
- **Standort:** Die Kontaktstelle muss sich nicht unbedingt innerhalb der EU befinden.
- **Kommunikation:** Die Sprache, in der mit der Kontaktstelle zu kommunizieren ist, sollte in den Informationen über deren Verfügbarkeit angegeben werden. Um die Kommunikation zwischen den HSPs und den zuständigen Behörden der Mitgliedstaaten zu ermöglichen, sollte

mindestens eine Amtssprache der EU verwendet werden. Dies sollte eine Sprache sein, in der auch die Nutzungsbedingungen der Plattform verfügbar sind.

Gesetzliche:r Vertreter:in ([TCO-Verordnung, Art. 17](#))

- **Notwendigkeit:** Wenn ein HSP keine Hauptniederlassung in der EU hat, muss ein:e gesetzliche:r Vertreter:in benannt werden. Dies ist eine natürliche oder juristische Person, die in einem der EU-Mitgliedstaaten ansässig ist, in denen der HSP seine Dienstleistungen anbietet.
- **Zweck:** Diese:r gesetzliche Vertreter:in ist für die Entgegennahme, Einhaltung und Durchsetzung der TCO-Verordnung und insbesondere der Entfernungsanordnungen zuständig.
- **Erforderliche Ressourcen:** HSPs müssen ihre gesetzlichen Vertreter:innen mit den erforderlichen Befugnissen, Kapazitäten und Ressourcen ausstatten, um die TCO-Verordnung einzuhalten und mit den zuständigen Behörden zusammenzuarbeiten.
- **Haftung:** Die gesetzlichen Vertreter:innen können für Verstöße gegen die TCO-Verordnung haftbar gemacht werden.
- **Verhältnis zur Kontaktstelle:** Der oder die gesetzliche Vertreter:in kann auch gleichzeitig als Kontaktstelle fungieren, ist aber nicht dazu verpflichtet, dies zu tun.

2. Warum ist eine Kontaktstelle oder ein:e gesetzliche:r Vertreter:in notwendig?

In den anderen Kapiteln werden viele Möglichkeiten und Maßnahmen erörtert, die für HSPs auch aus geschäftlicher Sicht interessant sein können. Der Hauptgrund und das Hauptargument für die **Einrichtung von Kontaktstellen oder die Benennung von gesetzlichen Vertreter:innen** ist schlicht und ergreifend, dass dies **obligatorisch** ist. Dies mag zwar eine gewisse Umverteilung von Ressourcen mit sich bringen, aber es liegt zweifellos im besten Interesse des HSPs, das Gesetz einzuhalten und die negativen Folgen der Nichteinhaltung, wie den Verlust von Ansehen, Vertrauen und Geld, falls Geldstrafen verhängt werden, zu vermeiden, indem die Benennung umgehend erfolgt.

HSPs müssen den zuständigen Behörden die Möglichkeit geben, die Informationen über die Kontaktstelle einzusehen und anschließend elektronische Meldungen zu übermitteln (d. h. eine Entfernungsanordnung elektronisch zu übermitteln). Dazu gehört in der Regel die Angabe einer E-Mail-Adresse (z. B. im Abschnitt „Kontakt“ auf der Webseite des HSPs), über die die zuständige Behörde die Kontaktstelle erreichen kann.

Bei der Ernennung von gesetzlichen Vertreter:innen sind zwei Aspekte hervorzuheben. Erstens muss die **Identität des gesetzlichen Vertreters bzw. der gesetzlichen Vertreterin bekannt gemacht werden** (siehe Kontaktstelle). Zweitens muss der HSP seine **Heimatbehörde** (d. h. die zuständige Behörde des Mitgliedstaats, in dem der oder die gesetzliche Vertreter:in niedergelassen ist) **aktiv über die Benennung informieren**.

Europol hat auch eine Plattform, [Plateforme Européenne de Retraits de Contenus illicites sur Internet](#) (Europäische Plattform für die Entfernung illegaler Inhalte im Internet), oder PERCI, entwickelt, um die Umsetzung der TCO-Verordnung zu erleichtern. Mit PERCI soll sichergestellt werden, dass HSPs Entfernungsanordnungen aus den EU-Mitgliedstaaten über einen gemeinsamen sicheren Kanal erhalten können, anstatt über 27 separate Systeme pro Mitgliedstaat. Das System vereinfacht die Bearbeitung

von Entfernungsanordnungen aus verschiedenen EU-Mitgliedstaaten und fungiert als zentrale Anlaufstelle für Empfehlungen und Entfernungsanordnungen, um die doppelte oder mehrfache Übermittlung von Entfernungsanordnungen, d. h. ein und dieselbe Entfernungsanforderung aus zwei oder mehreren EU-Mitgliedstaaten zu erhalten, zu verhindern. Außerdem macht PERCI auch die Arbeit für HSPs leichter, weil sie eine zentrale Anlaufstelle für Entfernungsanordnungen darstellt. Zudem dient PERCI dazu, die im Laufe der Zeit eingegangenen Entfernungsanordnungen und Empfehlungen zentral zu erfassen, um die Verpflichtung zur Transparenzberichterstattung zu unterstützen. Über PERCI können HSPs auch eine Prüfung und Überprüfung beantragen, um eine Entfernungsanordnung anzufechten.

3. Was ist die zuständige Behörde eines EU-Mitgliedstaates und wie kann ich mit ihr Kontakt aufnehmen?

Die Kontaktaufnahme mit der zuständigen Behörde, beispielsweise zur Mitteilung der gesetzlichen Vertreter:innen, ist unter bestimmten Umständen erforderlich. Ein solcher Umstand liegt auch dann vor, wenn eine Entfernungsanordnung angefochten werden soll. Ein weiterer Fall wäre beispielsweise, wenn ein HSP Kenntnis von terroristischen Inhalten erhält, die eine unmittelbare Bedrohung für das Leben oder eine terroristische Handlung darstellen, ohne dass eine Entfernungsanordnung vorliegt. In diesem Fall ist der HSP dazu verpflichtet, den Inhalt unverzüglich zu löschen und die zuständige Behörde des betroffenen EU-Mitgliedstaates zu informieren ([TCO-Verordnung, Art. 14.5](#)).

Die meisten zuständigen Behörden der EU-Mitgliedstaaten haben bereits Kontaktstellen eingerichtet. Eine aktuelle Liste mit Kontaktangaben finden Sie auf der Website der Europäischen Kommission [hier](#).

Kapitel 5

Aufbau eines Benachrichtigungs- und Beschwerdesystems für entfernte Inhalte



Zusammenfassung: Inhalt und Kernpunkte dieses Kapitels

- Betroffene **Nutzer:innen können im Rahmen von Beschwerdeverfahren Einspruch gegen Entfernungsanordnungen** (und, falls erforderlich gegen andere proaktive Moderationsmaßnahmen zur Durchsetzung der Nutzungsbedingungen) **einlegen**.
- Beschwerdeverfahren sind als **Kontroll- und Feedback-Mechanismus** wichtig, und zwar aus der Sicht der Nutzer:innen, der Unternehmen und des Gesetzgebers.
- HSPs müssen einen „wirksamen und zugänglichen“ Beschwerdemechanismus einrichten ([TCO-Verordnung, Art. 10.1](#)).
- Gemäß der TCO-Verordnung müssen die Beschwerdesysteme bestimmte inhaltliche und technische Anforderungen erfüllen.
- Ein Beschwerdeverfahren kann zu zwei verschiedenen Ergebnissen führen, nämlich (1) der Beschwerde wird stattgegeben, weil festgestellt wird, dass der Inhalt fälschlicherweise gesperrt wurde, oder (2) die Beschwerde wird abgewiesen, weil festgestellt wird, dass der Inhalt zu Recht gesperrt wurde.
- Je nach Ausgang des Beschwerdeverfahrens können die Inhalte Gegenstand anderer Maßnahmen sein.
- Dieses Kapitel enthält außerdem Leitlinien für die Gestaltung und Umsetzung eines HSP-spezifischen Beschwerdeverfahrens.

Beschwerdeverfahren ermöglichen es den Nutzer:innen, die Entfernung von Inhalten durch Kommunikation mit dem HSP anzufechten, und sind damit **der erste Schritt zur (rechtlichen) Anfechtung einer Entfernungsanordnung**. Mehr über das Beschwerdeverfahren erfahren Sie in ► [Kapitel 2](#).

1. Warum ist es notwendig, einen transparenten Beschwerdemechanismus einzurichten?

Es ist wichtig, einen Beschwerdemechanismus einzurichten, insbesondere aus (a) rechtlicher Sicht, (b) aus Sicht der Nutzer:innen und (c) aus Sicht des Unternehmens.

a) Rechtliche Perspektive

Durch Beschwerdeverfahren kommt ein HSP den **gesetzlichen Regelungen, die solche Mechanismen erforderlich machen**, entgegen. So schreibt die TCO-Verordnung ([Art. 10](#)) vor, dass HSPs einen wirksamen und zugänglichen Beschwerdemechanismus einrichten müssen, um Nutzer:innen die Möglichkeit

zu geben, die Entfernung oder Sperrung von Inhalten anzufechten. Nach der TCO-Verordnung muss der oder die Inhaltsanbieter:in innerhalb von zwei Wochen über das endgültige Ergebnis informiert werden.

b) Perspektive der Nutzer:innen

Ein Beschwerdemechanismus ist nicht nur eine rechtliche Anforderung. Ein klarer und zugänglicher Beschwerdemechanismus trägt dazu bei, Vertrauen bei den Nutzer:innen aufzubauen – sowohl bei denjenigen, deren Inhalte moderiert wurden, als auch und insbesondere bei den nicht betroffenen Nutzer:innen, die die Plattform wie vorgesehen verwenden. Auf diese Weise zeigen HSPs, dass sich die Nutzer:innen auf die Moderationsprozesse verlassen können, dass diese Prozesse auf einem **Verantwortungsgefühl gegenüber den Nutzer:innen beruhen** und dass die Plattformen **Grundrechte** wie die Meinungs- und Informationsfreiheit berücksichtigen.

c) Perspektive des Unternehmens

Beschwerdemechanismen können eine hilfreiche Form der **Selbstkontrolle** sein, bei der Moderationsmaßnahmen und -standards auf ihre Wirksamkeit, Fairness und Konsistenz geprüft werden. Solche Mechanismen können sicherstellen, dass Ihre Plattform so genutzt wird, wie es beabsichtigt ist, was wiederum dazu beiträgt, den **Ruf** Ihres HSPs zu schützen und das Recht auf freie Meinungsäußerung im Internet zu wahren.

2. Was sind die Anforderungen an ein Beschwerdesystem?

Gemäß der TCO-Verordnung ([33](#) & [Art. 10](#)) sollten die Beschwerdesysteme:

- benutzerfreundlich sein,
- wirksam und (leicht) zugänglich sein,
- sicheren Rahmen schaffen für die rasche und transparente Bearbeitung von Beschwerden, so dass der oder die Beschwerdeführer:in innerhalb von zwei Wochen über das Ergebnis der Überprüfung informiert wird.

Die Beschwerdesysteme müssen für die Zwecke der TCO-Verordnung eingerichtet werden, um fälschlicherweise entfernte Inhalte wiederherzustellen. Beschwerden können jedoch darüber hinaus auch gegen Maßnahmen zur Durchsetzung der Nutzungsbedingungen der Plattform außerhalb des Anwendungsbereichs der TCO-Verordnung verwendet werden.

3. Wie wird mit Beschwerden umgegangen und was sind die möglichen Folgen?

Sobald das Beschwerdesystem eingerichtet ist und ein:e Nutzer:in eine Beschwerde eingereicht hat, **prüft der HSP die Beschwerde und teilt dem oder der Beschwerdeführer:in die Entscheidung innerhalb von höchstens zwei Wochen mit, sofern es sich um Fälle handelt, die unter die TCO-Verordnung fallen.**

Es gibt zwei mögliche Ergebnisse des Überprüfungsverfahrens, die in der folgenden Tabelle aufgeführt sind.

<i>Ergebnis A</i>	<i>Ergebnis B</i>
Der Beschwerde eines Nutzers bzw. einer Nutzerin gegen die Entfernung des Inhalts wird stattgegeben.	Die Beschwerde eines Nutzers oder einer Nutzerin gegen die Entfernung des Inhalts wird abgewiesen.
Ergebnis: Die Beschwerde gegen die Entfernung des Inhalts ist berechtigt und wird daher zugelassen.	Ergebnis: Die Beschwerde gegen die Entfernung des Inhalts ist nicht gerechtfertigt und wird daher zurückgewiesen.
Bedeutet: Der Inhalt wurde unzulässigerweise entfernt, gelöscht oder anderweitig moderiert.	Bedeutet: Der Inhalt wurde ordnungsgemäß entfernt, gelöscht oder anderweitig moderiert.
Weiteres Verfahren: Der HSP (1) teilt dem oder der Beschwerdeführer:in das Ergebnis der Überprüfung mit und (2) stellt den Inhalt wieder her.	Weiteres Verfahren: Der HSP (1) informiert den oder die Beschwerdeführer:in über das Ergebnis der Überprüfung und (2) teilt ihm bzw. ihr die Gründe für diese Entscheidung mit.

4. Praktische Tipps und Ratschläge: Welche Elemente sind beim Aufbau eines Beschwerdesystems sinnvoll?

Dass ein Beschwerdesystem über bestimmte Funktionen verfügen muss, ist nicht nur eine Anforderung des Gesetzes, sondern auch der **Benutzerfreundlichkeit**.

Wie auch bei anderen wichtigen Fragen wie den Nutzungsbedingungen (► [Kapitel 1](#)), der Einrichtung eines Verfahrens zur Identifizierung verbotener Inhalte (► [Kapitel 2](#)) oder der Wahl plattformspezifischer Moderationsmechanismen (► [Kapitel 3](#)) kann das System zur Einreichung einer Beschwerde von Plattform zu Plattform sehr unterschiedlich sein. Während einige Plattformen die Möglichkeit bieten, Beschwerden per E-Mail einzureichen, entscheiden sich andere für standardisierte, formularbasierte Online-Anwendungen. **Beschwerdesysteme sollten auf den Zweck, die Struktur und die Organisation einer Plattform zugeschnitten sein.** Einige Anregungen zur Einrichtung eines Beschwerdesystems finden Sie in der folgenden **Checkliste**.



Geben Sie klare Informationen über die Entfernung von Inhalten

Benachrichtigen Sie die Person, deren Inhalt entfernt wurde. Dies sollte auch dann erfolgen, wenn der Inhalt auf andere Weise moderiert wurde. Informieren Sie die Person in diesem Zusammenhang auch darüber, warum der Inhalt entfernt wurde (siehe den folgenden Punkt zu pädagogischen Hintergrundinformationen) und wie gegen die Entscheidung zur Entfernung Einspruch eingelegt werden kann (siehe den folgenden Punkt zur Erläuterung des Beschwerdeverfahrens).



Erklären Sie das Beschwerdeverfahren

Erklären Sie Ihren Nutzer:innen das Beschwerdeverfahren. Dies sollte im Zuge der Benachrichtigung darüber geschehen, dass Inhalte entfernt oder anderweitig moderiert wurden. Informationen über das Beschwerdeverfahren können auch in die Nutzungsbedingungen aufgenommen werden. Die Erläuterung des Beschwerdeverfahrens sollte Folgendes beinhalten: (1) wie Beschwerden eingereicht werden können, (2) wie das Überprüfungsverfahren abläuft und (3) wie die Nutzer:innen über das Ergebnis der Überprüfung informiert werden.



Stellen Sie pädagogische Hintergrundinformationen bereit

Geben Sie den Nutzer:innen die Möglichkeit zu erfahren, warum der Inhalt entfernt wurde und gegen welche Bestimmungen er verstößt – erklären Sie dies also (kurz). Der Inhalt kann beispielsweise entfernt werden, wenn er gegen die Nutzungsbedingungen verstößt oder wenn eine zuständige Behörde im Rahmen der TCO-Verordnung die Entfernung verlangt hat. Im ersten Fall kann diese Information durch Hinzufügen der plattformspezifischen Verbote der Nutzungsbedingung (z. B. gegen Hassrede, Anstiftung zur Gewalt, sexuelle Inhalte und Belästigung) spezifiziert werden. Im letzteren Fall empfiehlt es sich, dem Beschwerdesystem einen kurzen informativen Überblick über die TCO-Verordnung hinzuzufügen, damit der rechtliche Rahmen für die Nutzer:innen klar wird.



Informieren Sie die Nutzer:innen regelmäßig über den Stand der Beschwerde

Die Nutzer:innen sollten regelmäßig über den Stand und den Fortschritt der Beschwerde informiert werden. Diese Aktualisierungen sollten zumindest aus einer Benachrichtigung über den Abschluss der Prüfung und einer rechtzeitigen Mitteilung des Ergebnisses bestehen. Eine ausführlichere Mitteilung könnte den oder die Nutzer:in darüber informieren, dass die Beschwerde eingegangen ist und nun von HSP-Mitarbeiter:innen geprüft wird. Eine bewährte Praxis ist es, dem oder der Nutzer:in einen groben Zeitplan für die Bearbeitung seiner Beschwerde zu geben. Solche Statusupdates können per E-Mail erfolgen oder in einem Online-Portal angezeigt werden.



Dokumentieren Sie den (individuellen) Beschwerdeprozess

Es ist wichtig, den Beschwerdeprozess zu dokumentieren. Die Dokumentation dient als Referenz für spätere Fragen oder Streitigkeiten.

Kapitel 6

Praktische Unterstützung und Ratschläge zur Transparenzberichterstattung



Zusammenfassung: Inhalt und Kernpunkte dieses Kapitels

- Transparenzberichte ermöglichen es HSPs, **öffentlich zu kommunizieren**, wie ihre **Werte** auf der Plattform gelebt werden und welche **Maßnahmen gegen verbotene und illegale Inhalte und Verhaltensweisen ergriffen wurden**.
- Transparenzberichte sind ein **wichtiges Instrument, um öffentliche Verantwortung zu übernehmen und Glaubwürdigkeit und Vertrauenswürdigkeit zu demonstrieren**.
- Verschiedene **Gesetze**, darunter die TCO-Verordnung, **verlangen** ausdrücklich eine **Transparenzberichterstattung**.
- Bei der Erstellung von Transparenzberichten ist es ratsam, vor, während und nach dem Prozess systematisch vorzugehen und bestimmte Schritte einzuhalten.
- Die **TCO-Verordnung verlangt von HSPs, die terroristischen Inhalten ausgesetzt sind oder gegen sie vorgegangen sind, einen jährlichen Transparenzbericht über ihre Aktivitäten in Bezug auf terroristische Inhalte zu veröffentlichen**. Der Bericht muss bestimmte wesentliche Zahlen und Informationen enthalten, z. B. die Anzahl der eingegangenen Entfernungsanordnungen und die Anzahl der entfernten Inhalte. Der Bericht muss bis spätestens 1. März des Folgejahres veröffentlicht werden ([TCO-Verordnung, Art. 7.2](#)).

1. Was sind Transparenzberichte?

Transparenzberichte sind ein **wichtiges Instrument für HSPs, um ihre Rechenschaftspflicht, Glaubwürdigkeit und Vertrauenswürdigkeit unter Beweis zu stellen und gesellschaftlich relevante Informationen zu veröffentlichen**. Transparenzberichte **enthalten wichtige Daten über Anfragen, die HSPs von staatlichen Akteur:innen weltweit erhalten, und darüber, wie diese Anfragen bearbeitet wurden**, was die Zusammenarbeit und Kooperation mit Behörden und anderen staatlichen Stellen transparent machen soll⁷.

Transparenzberichte geben auch einen Überblick darüber, welche Maßnahmen der HSP zur Durchsetzung von Vorschriften ergriffen hat (z. B. durch die Entfernung von Inhalten oder andere Maßnahmen

⁷ Urman, A., & Makhortykh, M. (2023). How transparent are transparency reports? Comparative analysis of transparency reporting across online platforms. *Telecommunications Policy*, 47(3), 102477. <https://doi.org/10.1016/j.telpol.2022.102477>

der Moderation). Dies umfasst die Durchsetzung von (1) plattformspezifischen Richtlinien (in der Regel Nutzungsbedingungen; ► [Kapitel 1](#)), (2) Rechten wie dem Urheber- oder Markenrecht und (3) (lokalen) Gesetzen und Vorschriften, die zur Entfernung von Inhalten führen⁸. In der EU gehören zu den lokalen Rechtsvorschriften die TCO-Verordnung und der DSA. Auch länderspezifische Rechtsvorschriften können von Bedeutung sein, wie beispielsweise das Netzwerkdurchsetzungsgesetz in Deutschland.

Transparenzberichte werden normalerweise regelmäßig veröffentlicht. Die TCO-Verordnung setzt fest, dass dies **(mindestens) einmal pro Jahr geschehen** sollte, wenn ein HSP Maßnahmen gegen terroristische Inhalte ergriffen hat oder ergreifen musste ([TCO-Verordnung, 30](#)).

Die Transparenzberichte und die darin ausgewiesenen Kennzahlen können von HSP zu HSP sehr unterschiedlich sein⁹. **Für Transparenzberichte im Sinne der TCO-Verordnung gibt es spezifische Anforderungen, welche Informationen enthalten sein müssen.** Mehr dazu erfahren Sie in ► [Abschnitt 4 dieses Kapitels](#).

2. Warum sind Transparenzberichte notwendig?

Transparenzberichte **ermöglichen es Nutzer:innen und Dritten zu beurteilen, inwieweit HSPs ihren eigenen Grundsätzen, rechtlichen Anforderungen, dem Datenschutz und dem Schutz der Privatsphäre treu bleiben**⁶. Sehen wir uns die verschiedenen Perspektiven an, warum Transparenzberichte wichtig sind.

a) Rechtliche Perspektive

Transparenzberichte sind nützlich und oft notwendig, um EU-Verordnungen wie die TCO-Verordnung, den DSA und gegebenenfalls länderspezifische Gesetze einzuhalten. Wenn HSPs innerhalb eines Kalenderjahres Maßnahmen gegen die Verbreitung terroristischer Inhalte ergriffen haben, sei es proaktiv oder aufgrund einer Entfernungsanordnung, **muss bis spätestens 1. März des Folgejahres** ein Transparenzbericht **veröffentlicht werden** ([TCO-Verordnung, Art. 7.2](#)). Dies bedeutet, dass die Transparenzberichte eher verpflichtend sind als nicht. Die zuständigen Behörden sind auch verpflichtet, jährliche Transparenzberichte zu veröffentlichen ([TCO-Verordnung, 31](#)).

b) Perspektive der Nutzer:innen und Stakeholder

Transparenzberichte helfen den Nutzer:innen und anderen Beteiligten zu beurteilen, inwieweit der HSP seiner **Verantwortung gegenüber der Gesellschaft gerecht** wird. Gleichzeitig trägt die regelmäßige Veröffentlichung von Transparenzberichten dazu bei, dass der HSP **Vertrauen und einen guten Ruf in der Öffentlichkeit aufbauen kann**, indem er Compliance, Engagement und Zuverlässigkeit demonstriert.

⁸ Trust & Safety Professional Association (2023). What Is A Transparency Report? TSPA. <https://www.tspa.org/curriculum/ts-fundamentals/transparency-report/what-is-a-transparency-report/>

⁹ Woolery, L., Budish, R., & Bankston, K. (2016). The transparency reporting toolkit. *New America and The Berkman Center for Internet & Society at Harvard University*.

c) Perspektive des Unternehmens

Ähnlich wie Beschwerdemechanismen können Transparenzberichte auch ein **Instrument zur Selbstkontrolle** sein, das Bereiche aufzeigt, in denen die Geschäftsprozesse optimiert werden können. Da kleine(re) Internetdienstleister bei terroristischen Akteuren besonders beliebt sind (nähere Informationen finden Sie in [diesem Bericht von Tech Against Terrorism](#)), ist es für sie besonders wichtig, gegen die Verbreitung terroristischer Inhalte vorzugehen. Transparenzberichte sind eine Möglichkeit für kleine(re) HSPs, ihr Engagement in diesem Bereich zu demonstrieren.

3. Ein Prozess für die Erstellung von Transparenzberichten

Die erstmalige Erstellung und Veröffentlichung eines Transparenzberichts kann eine entmutigende Aufgabe sein. Sobald jedoch ein **Prozess und eine Routine für die Erstellung jährlicher Transparenzberichte** etabliert sind, muss die Struktur des Berichts in der Regel nicht mehr komplett überarbeitet werden, und Aktualisierungen sind normalerweise ausreichend. In diesem Leitfaden wird ein Beispielprozess erläutert, wie ein Transparenzbericht aus der Sicht des HSPs erstellt werden kann und was im Vorfeld, während und nach der Erstellung zu beachten ist.

a) Vor der Erstellung des Transparenzberichts

Scannen Sie die gesetzliche Landschaft

Verschaffen Sie sich einen Überblick über die gesetzlichen Regelungen, die für Ihren HSP gelten. So sind beispielsweise die TCO-Verordnung und der DSA EU-weit relevant. Möglicherweise gibt es länderspezifische Vorschriften sowie Anforderungen für andere Themen, die für Ihren HSP relevant sind, abgesehen von terroristischen Inhalten. Wenn Sie Ansprechpartner:innen oder Anwält:innen im Unternehmen haben, ist es oft ratsam, sich mit diesen auszutauschen, um festzustellen, welche Vorschriften (abgesehen von der TCO-Verordnung, um die es hier geht) für Ihren HSP gelten.

Bestimmen Sie die Ziele des Transparenzberichts

Überlegen Sie, was die Ziele Ihres Transparenzberichts sind. Wichtige Fragen, die Ihnen dabei helfen können, sind: Wollen Sie einfach ‚nur‘ Ihre rechtlichen Verpflichtungen erfüllen oder wollen Sie auch andere Themen und Ihr Engagement dafür thematisieren? Wen wollen Sie erreichen, d.h. welche Zielgruppe ist für Ihren HSP sinnvoll (z.B. politische Akteur:innen, Nutzer:innen, Geldgeber:innen)? Wie oft wollen Sie Transparenzberichte veröffentlichen und was ist der beste Zeitpunkt für Ihr jeweiliges Geschäftsjahr?

Bestimmen Sie, welche Daten einbezogen werden können und müssen

Legen Sie fest, welche Daten Sie in den Transparenzbericht aufnehmen wollen. Einerseits ist dafür das *Können* relevant, d.h. welche Daten sind vorhanden bzw. für welche ist es denkbar, dass Sie sie in Zukunft erheben können? Zum anderen ist das *Müssen* entscheidend, d.h.: welche

gesetzlichen Anforderungen müssen Sie erfüllen und welche Daten sind dafür notwendig? Welche Informationen und Daten Sie nach der TCO-Verordnung aufnehmen müssen, erfahren Sie im ► [nächsten Unterkapitel](#).

b) Während der Erstellung des Transparenzberichts

Verwenden Sie eine klare und prägnante Sprache

Achten Sie bei der Erstellung des Transparenzberichts darauf, dass eine klare und präzise Sprache verwendet wird. Dies erleichtert die Auseinandersetzung mit und das Verständnis von komplexem Material. Die Sprache sollte außerdem an die vorgesehene Leser:innenschaft angepasst werden.

Bereiten Sie kontextbezogene Informationen und Erklärungen auf

Geben Sie Ihren Leser:innen kontextbezogene Informationen und Erklärungen an die Hand. Solche Erklärungen ermöglichen es den Nutzer:innen, die Funktionsweise Ihrer HSP besser zu verstehen und zu begründen, warum sie (vielleicht) einen detaillierteren Transparenzbericht liefert als ‚nur‘ einen Bericht, der lediglich die regulatorischen Mindestanforderungen erfüllt.

Beziehen Sie internes Feedback ein

Bei der Planung eines Transparenzberichts sollten Sie Feedback-Runden in den Zeitplan für die Erstellung einbeziehen. Regelmäßige Rückmeldungen und Korrekturen am Inhalt und an der Sprache des Berichts können für alle Beteiligten wertvoll sein, insbesondere für diejenigen, die mit der Erstellung des Berichts beauftragt sind.

c) Nach der Erstellung des Transparenzberichts

Veröffentlichen Sie den Transparenzbericht

Überlegen Sie, in welchen Sprachen Sie den Transparenzbericht veröffentlichen wollen, und erstellen Sie entsprechende Übersetzungen. Legen Sie auch fest, wo er zugänglich sein soll, d. h. beispielsweise wo auf Ihrer Webseite. Darüber hinaus können Sie auch erwägen, den Transparenzbericht in verschiedene Kommunikationsmaterialien einzubinden, um ihm zu mehr Aufmerksamkeit zu verhelfen. Dazu könnte gehören, dass Sie ihn auf Ihrer Webseite einbetten, ihn in E-Mail-Newslettern verschicken oder ihn in sozialen Medien teilen.

Aktualisieren Sie die Daten und schließlich den Transparenzbericht regelmäßig

Wenn der erste Transparenzbericht fertiggestellt ist, haben Sie bereits die Grundlage geschaffen, die den nächsten Bericht erleichtern wird, da dieser nun als Vorlage genutzt werden kann. Das Verfahren zur Sammlung relevanter Daten im Laufe des Jahres und deren Organisation, damit sie leicht abrufbar sind, wird die Erstellung des nächsten Transparenzberichts erleichtern und weniger zeit- und ressourcenintensiv machen.

Lassen Sie Raum für Verbesserungen

Seien Sie offen für Änderungen und Anpassungen. Wenn Sie externes Feedback erhalten, sollten Sie es gegebenenfalls in den nächsten Transparenzbericht einfließen lassen. Relevantes Feedback kann jedoch nicht nur von außen kommen. Nach der Veröffentlichung kann der HSP auch einen kritischen Blick auf den vorangegangenen Transparenzbericht, die Kommunikation rund um ihn und die Reaktionen darauf werfen, indem Presseerklärungen oder andere relevante Quellen berücksichtigt werden. Sowohl internes als auch externes Feedback kann Aufschluss darüber geben, wo möglicherweise Verbesserungsbedarf besteht.

4. Welche Informationen und Kennzahlen müssen gemäß TCO-Verordnung in den Transparenzbericht aufgenommen werden?

Die TCO-Verordnung erläutert in [Artikel 7.3](#) die **Mindestanforderungen für Transparenzberichte**, d.h. was genau enthalten sein muss, um dieser EU-Verordnung zu entsprechen. Wir stellen diese Anforderungen im Folgenden in einer Checkliste vor:

1) **Informationen** darüber, welche Maßnahmen der HSP ergriffen hat:

- ☒ um terroristische Inhalte zu identifizieren;
- ☒ um terroristische Inhalte zu entfernen oder zu deaktivieren;
- ☒ um das erneute Auftauchen und Hochladen von zuvor gesperrtem Online-Material zu verhindern (dies ist besonders wichtig, wenn automatisierte Verfahren eingesetzt werden).

2) **Kennzahlen** und ggf. zusätzliche Informationen über die Anzahl der:

- ☒ entfernten Artikel mit terroristischem Inhalt (aufgrund von Entfernungsanordnungen oder anderen Maßnahmen);
- ☒ Entfernungsanordnungen, die nicht umgesetzt wurden, und zusätzliche Informationen darüber, warum dies nicht der Fall war;
- ☒ Beschwerden, die vom HSP über den Beschwerdemechanismus bearbeitet wurden, sowie zusätzliche Informationen über das Ergebnis der Beschwerden;
- ☒ Fälle, in denen der HSP den Inhalt nach einer Beschwerde durch den oder die Inhaltsanbieter:in wiederhergestellt hat;
- ☒ von der HSP eingeleitete Gerichtsverfahren und zusätzliche Informationen über den Ausgang dieser Verfahren;
- ☒ Fälle, in denen die HSP nach Gerichtsverfahren Inhalte wiederherstellen musste.

C. Vielen Dank für Ihre Hilfe bei der Bekämpfung der terroristischen Bedrohung!

Herzlichen Glückwunsch!

Sie haben es bis hierher geschafft, und das bedeutet, dass Sie wichtige Kenntnisse über die Anforderungen der TCO-Verordnung und weitere Maßnahmen zur Bekämpfung terroristischer und anderer schädlicher Inhalte im Internet erworben haben. Auf diese Weise tragen Sie zu einem sichereren Internet bei.

Wir sind uns bewusst, dass die Umsetzung dieser Maßnahmen viel Aufmerksamkeit und Ressourcen erfordert. Die Tatsache, dass Sie sich mit diesem Leitfaden befassen haben, ist ein großer Schritt, und wenn dieser Leitfaden Ihnen hilft, über eine Strategie zur Umsetzung der Maßnahmen gegen terroristische Inhalte nachzudenken, die für Ihren HSP geeignet ist, dann haben wir schon viel erreicht! Wir sind zuversichtlich, dass dieser Leitfaden zusammen mit unseren anderen Materialien eine Ressource sein wird, die Ihnen und Ihrem HSP dabei helfen kann, den Verpflichtungen im Hinblick auf die Bekämpfung der terroristischen Online-Bedrohung nachzukommen.

Vielen Dank für Ihr Engagement bei der Bekämpfung der terroristischen Bedrohung im Internet und dafür, dass Sie sich für Ihre HSP und Ihre Nutzer:innen einsetzen.



PS: Das TATE-Projekt umfasst auch einen **kostenlosen Online-Kurs**, in dem Anforderungen und die Einhaltung der europäischen TCO-Verordnung vertieft werden. In diesem Kurs können Sie tiefer in die Materie eintauchen und finden Details zur Verordnung, Beispiele dafür, wie andere Plattformen einzelne Maßnahmen umsetzen, und allgemeinere Informationen über terroristisches Verhalten im Internet. **Nach erfolgreichem Abschluss des Kurses erhalten Sie ein offizielles Zertifikat, das von renommierten Universitäten (LMU München, Universität Gent) ausgestellt wird.** Zusätzlich bietet TATE ein Capacity Building Programm an, in dem HSPs praktische Unterstützung für die Anforderungen im Zusammenhang mit der TCO-Verordnung erhalten können.

D. Glossar

Begriff	Erläuterung
Entfernungsanordnung	Eine Aufforderung, die ein HSP von einer zuständigen Behörde erhält. Sie informiert den HSP darüber, dass terroristische Inhalte auf der Plattform verbreitet wurden, und verpflichtet den HSP, diese innerhalb einer Stunde nach Eingang der Anordnung zu entfernen.
HSP	Hosting Service Provider; die TCO-Verordnung gilt für HSPs. Weitere Einzelheiten darüber, welche HSPs in den Anwendungsbereich der TCO-Verordnung fallen, finden Sie ► hier .
Inhalteanbieter:in	Die Person, die Inhalte auf der jeweiligen Plattform bereitstellt, also beispielsweise einen Beitrag veröffentlicht.
Nutzungsbedingungen	Von der Plattform aufgestellte verbindliche Regeln, die (1) den Umfang und die Verantwortung der HSP gegenüber den Nutzer:innenn und (2) angemessene und erlaubte, aber auch verbotene Nutzungspraktiken festlegen. Die Nutzer:innen müssen sie einhalten, wenn sie den den angebotenen Dienst weiterhin nutzen wollen. Im Englischen werden Nutzungsbedingungen häufig als Terms of Service (abgekürzt: ToS) bezeichnet. Es gibt zahlreiche Synonyme wie Terms of Use, Terms and Conditions oder Community Standards.
PERCI	Ein von Europol koordiniertes Tool, das die Kommunikation zwischen HSPs und zuständigen Behörden verbessern und erleichtern soll.
TCO	Terrorist Content Online (dt.: terroristische Inhalte im Internet); Inhalte, die terroristische Elemente enthalten oder zur Förderung terroristischer Zwecke bestimmt sind. Eine ausführliche Definition findet sich in der ► Einleitung . Terroristische Online-Inhalte stehen in engem Zusammenhang mit ► Terroristischen Straftaten , die sehr unterschiedlicher Natur sein können.
TCO-Verordnung (auch: LEX 2021/784 & Verordnung zur Bekämpfung der Verbreitung terroristischer Online-Inhalte)	Die EU-Verordnung gegen die Verbreitung terroristischer Inhalte im Internet, die im Jahr 2022 in Kraft tritt. Sie gilt für Hosting Service Provider (HSPs), die ihre Dienste in der EU anbieten.
Zuständige Behörden	Die Behörden eines EU-Mitgliedstaates, die für die Umsetzung der TCO-Verordnung zuständig sind. Eine Übersicht über die jeweils zuständigen Behörden der EU-Mitgliedstaaten finden Sie hier .