Projektpartner:

Co-funded by
the European Union

Informationsblatt für Jugendorganisationen mit Berichtsfunktion:

Wie man im Rahmen des DSA mit Koordinatoren für digitale Dienste zusammenarbeitet

---

Einleitung und Zusammenfassung

Jugendorganisationen spielen heute eine entscheidende Rolle beim Schutz junger Menschen im Internet. Ob sie nun Hilfetelefone, Peer-Education-Programme, Beratungsstellen gegen Cybermobbing, Meldeportale für Hassrede oder umfassendere Initiativen zur digitalen Kompetenz betreiben – sie reagieren oft als erste auf Online-Gefahren. Die Organisationen erfahren in der Regel als Erste, wenn eine schädliche Challenge viral geht, eine neue Form der Belästigung auftaucht oder bestimmte Gruppen junger Menschen Zielscheibe von Hassrede oder Anbahnungsversuchen werden. Trotz dieser wichtigen Rolle war ihre Zusammenarbeit mit staatlichen Behörden und Online-Plattformen bisher oft informell, uneinheitlich und stark von persönlichen Beziehungen abhängig.

Das **Gesetz über digitale Dienste (Digital Services Act, DSA)** verändert diese Landschaft grundlegend. Es schafft klare Strukturen für die Plattformregulierung in der gesamten Europäischen Union und richtet in jedem Mitgliedstaat eine neue nationale Behörde ein – den **Koordinator für digitale Dienste (Digital Services Coordinator, DSC)** . Für Jugendorganisationen stellt die Einführung der DSCs eine historische Chance dar: Erstmals können sie formell Einfluss auf die Rechenschaftspflicht von Plattformen nehmen, zu Risikobewertungen beitragen, illegale Inhalte über anerkannte Kanäle melden und mit einer nationalen Behörde zusammenarbeiten, die die Befugnis hat, die Einhaltung der Plattformverpflichtungen durchzusetzen.

Dieses Informationsblatt bietet Jugendorganisationen einen praktischen Leitfaden für die effektive Zusammenarbeit mit digitalen Sicherheitszentren (DSCs). Es erläutert den rechtlichen Rahmen, das Mandat und die Struktur der DSCs sowie die besonderen Beiträge, die Jugendorganisationen leisten können. Darüber hinaus werden Meldeverfahren, die Zusammenarbeit in Krisensituationen, Grundsätze des Datenmanagements, Forschungskooperationen und langfristige strategische Partnerschaften beschrieben. Ziel ist es, jugendorientierte NGOs mit dem nötigen Wissen und praktischen Ansätzen auszustatten, um sich reibungslos in das neue Ökosystem der digitalen Sicherheitsinfrastruktur (DSA) zu integrieren und ihre Wirkung auf die digitale Sicherheit junger Menschen zu maximieren.

Co-funded by the European Union

Die DSA im Kontext: Warum sie für Jugendorganisationen wichtig ist

Der Digital Services Act (DSA) wurde geschaffen, um ein sichereres, transparenteres und verantwortungsvolleres digitales Umfeld in der gesamten EU zu gewährleisten. Für Jugendarbeiter sind drei Elemente des DSA besonders wichtig. Erstens führt der DSA strenge Regeln für den Umgang von Plattformen mit illegalen Inhalten ein, darunter Hassrede, Material mit sexuellem Kindesmissbrauch und Gewaltdrohungen und bestimmte Formen von Datenschutzverletzungen. Plattformen müssen es Nutzern und Organisationen ermöglichen, Meldungen einzureichen, diese schnell zu bearbeiten und Maßnahmen zu ergreifen, wenn die Inhalte tatsächlich rechtswidrig sind.

Zweitens führt der DSA **besondere Verpflichtungen zum Schutz von Minderjährigen ein** . Online-Plattformen müssen ihre Dienste so gestalten, dass sie den Interessen von Kindern bestmöglich gerecht werden, manipulative Gestaltungspraktiken vermeiden, standardmäßig hohe Datenschutzeinstellungen für Minderjährige gewährleisten und Risiken in Bezug auf psychische Gesundheit, Cybermobbing, Suchtverhalten, den Kontakt mit schädlichen Inhalten und Ausbeutung bewerten.

Drittens schafft die DSA eine mehrstufige Regulierungsstruktur. Die Europäische Kommission beaufsichtigt die größten Plattformen (VLOPs und VLOSEs), während die nationalen DSCs alle in ihrem Zuständigkeitsbereich aktiven Plattformen überwachen. Jugendorganisationen agieren naturgemäß auf lokaler oder nationaler Ebene und fügen sich daher logisch in das Kooperationsnetzwerk der DSCs ein. Ihre Beobachtungen, Fallstudien und direkten Interaktionen mit jungen Nutzern liefern wichtige Kontextinformationen, die den DSCs allein nicht zugänglich sind.

Aus diesem Grund fördert die DSA die strukturierte Zusammenarbeit zwischen nationalen Behörden und zivilgesellschaftlichen Akteuren. Jugendorganisationen haben dadurch die Möglichkeit, nicht nur im Einzelfall zur Online-Sicherheit beizutragen, sondern auch die Durchsetzung von Vorschriften, systemische Risikobewertungen und die Verantwortlichkeit von Plattformen mitzugestalten. Der Wert dieser Zusammenarbeit liegt in der Verbindung von Regulierungsbefugnissen mit praktischer Erfahrung – eine Kombination, die unerlässlich ist, um digitale Umgebungen für junge Nutzer sicherer zu machen.

- ## Digitale Servicekoordinatoren (DSCs) verstehen

Die neu eingerichteten Koordinatoren für digitale Dienste (Digital Services Coordinators, DSC) sind nationale Behörden, die für die Überwachung der Einhaltung des Digital Services Act (DSA) zuständig sind. Ihre Struktur kann je nach Mitgliedstaat variieren – einige sind in bestehende Regulierungsbehörden integriert, andere sind gänzlich neue Einrichtungen –, ihr Mandat ist jedoch EU-weit einheitlich. Ein DSC muss alle im Land angebotenen digitalen Dienste überwachen, potenzielle Verstöße untersuchen, trusted Flagger zertifizieren, mit der

Zivilgesellschaft und Forschern zusammenarbeiten und als zentrale Anlaufstelle für Plattformen und die Europäische Kommission fungieren.

Für Jugendorganisationen ist es hilfreich zu verstehen, wie digitale Sicherheitszentren (DSCs) intern arbeiten. Die meisten DSCs umfassen mindestens drei wichtige Abteilungen. Die erste ist die **Abteilung für Durchsetzung und Ermittlung** , die eingehende Meldungen prüft, Plattformen untersucht, Informationen anfordert und Durchsetzungsmaßnahmen entwickelt. Die zweite Abteilung ist die **Abteilung für Systemrisiko- und Plattformbewertung** , die prüft, ob Plattformen ihren Verpflichtungen zum Schutz von Minderjährigen und zur Eindämmung der Verbreitung illegaler oder schädlicher Inhalte nachkommen. Die dritte Abteilung ist die **Abteilung für Stakeholder- und Zivilgesellschaftsarbeit** , die die Zusammenarbeit mit Nichtregierungsorganisationen, Bildungseinrichtungen, Forschungsinstituten und öffentlichen Stellen koordiniert.

Jugendorganisationen können mit allen drei Abteilungen zusammenarbeiten. Beispielsweise würde eine NGO bei der Meldung eines schädlichen Vorfalls, der einen jungen Menschen betrifft, mit der Strafverfolgungsabteilung kommunizieren. Bei der Bereitstellung von Erkenntnissen zu systemischen Trends, wie etwa Cybermobbing-Mustern oder neu auftretenden Gefahren, könnten sie mit der Risikobewertungsabteilung zusammenarbeiten . Und bei der Teilnahme an öffentlichen Konsultationen, Kampagnen oder Arbeitsgruppen würden sie mit der Stakeholder-Abteilung zusammenarbeiten.

Das Verständnis dieser Strukturen hilft Jugendorganisationen dabei, zu wissen, an wen sie sich für verschiedene Formen der Zusammenarbeit wenden können und wie sie ihre Arbeit in etablierte Regulierungsprozesse integrieren können.

Warum Jugendorganisationen unverzichtbare Partner für DSCs sind

Obwohl die DSCs über weitreichende Regulierungsbefugnisse verfügen, fehlt ihnen etwas, das Jugendorganisationen besitzen: **der ständige, direkte Kontakt zu jungen Menschen und ihrem Umfeld** . Regulierungsbehörden betreiben keine Hotlines, Workshops, Schulprogramme oder Peer-Education-Initiativen. Sie erleben Cybermobbing-Fälle nicht in Echtzeit und verfolgen auch nicht die Trends auf TikTok, Discord oder Instagram aus der Perspektive junger Menschen. Jugendorganisationen hingegen sind täglich Zeugen dieser Dynamiken.

Dadurch entsteht eine natürliche Synergie. Digitale Beratungsstellen benötigen hochwertige, kontextbezogene und aktuelle Informationen über die Vorgänge auf den Plattformen – und Jugendorganisationen brauchen eine Autorität, die tatsächlich für Verantwortlichkeit sorgen kann. Junge Menschen erleben oft Schäden, die in den Transparenzberichten der Plattformen oder offiziellen Beschwerdemechanismen nicht vollständig erfasst werden. Jugendarbeiter verstehen, wie sich bestimmte Verhaltensweisen äußern, warum junge Menschen Inhalte auf eine bestimmte Weise interpretieren und welche spezifischen Schwachstellen Kinder und Jugendliche haben.

Eine Jugend-NGO könnte beispielsweise beobachten, dass ein scheinbar harmloses Meme-Format dazu verwendet wird, neurodiverse Schüler in privaten Gruppenchats gezielt anzusprechen. Ein DSC allein würde diesen Trend nicht erkennen, aber mit den Erkenntnissen der NGO kann es den Schaden einordnen, bewerten, ob Plattformen illegale Inhalte nicht ausreichend entfernen, und Plattformen auffordern, ihre Richtlinien oder Durchsetzungssysteme anzupassen.

Wenn neue schädliche Entwicklungen auftreten, erfahren Jugendorganisationen oft als Erste von Schülern davon. Plattformen reagieren unter Umständen langsam oder uneinheitlich, wenn keine Regulierungsbehörde eingreift. In solchen Fällen kann die NGO die DSC frühzeitig warnen und so eine schnellere und koordinierte Reaktion ermöglichen.

Kurz gesagt, verfügen Jugendorganisationen über Expertise und Situationsbewusstsein, die DSCs intern nicht nachbilden können. Die DSA erkennt dies an und fördert ausdrücklich die Zusammenarbeit, wodurch NGOs zu unverzichtbaren Partnern beim Schutz der Online-Umgebungen junger Menschen werden.

Wie Zusammenarbeit in der Praxis funktioniert: Kommunikation und Berichterstattung

Der grundlegendste Mechanismus der Zusammenarbeit zwischen Jugendorganisationen und digitalen Sicherheitszentren (DSCs) ist die **strukturierte Meldung illegaler oder schädlicher Inhalte** . Zwar können NGOs heute bereits Meldungen direkt an die Plattformen übermitteln, doch das DSA schafft zusätzliche Wege über die DSCs. Dies ist hilfreich, wenn Plattformen nicht angemessen reagieren, wenn ein Muster auf systemische Mängel hindeutet oder wenn der Schaden besonders schwerwiegend ist.

Um sicherzustellen, dass die DSCs effektiv handeln können, sollten Jugendorganisationen klare interne Verfahren zur Überprüfung von Inhalten, zur Dokumentation von Beweismitteln und zur Bereitstellung von Kontextinformationen entwickeln. Ein guter Bericht enthält: die URL des Inhalts, Screenshots mit Zeitstempeln, eine kurze Beschreibung der Situation, gegebenenfalls den relevanten rechtlichen Kontext und eine kurze Erläuterung, warum der Inhalt für den betroffenen Jugendlichen schädlich ist. Verfügt eine Organisation bereits über ein etabliertes Meldesystem, kann sie DSA-spezifische Felder in ihren Meldeprozess integrieren.

Sobald der Bericht beim DSC eingeht, prüft die Behörde dessen Gültigkeit und entscheidet, ob sie ihn an die Plattform weiterleitet, weitere Informationen anfordert oder eine umfassendere Untersuchung einleitet. Das DSC kann sich zur Klärung auch an die NGO wenden. Sobald die Plattformen antworten, informiert das DSC die NGO in der Regel über das Ergebnis. Dadurch entsteht mit der Zeit ein strukturierter Kommunikationskreislauf, der die Qualität und Konsistenz der Ergebnisse der Inhaltsmoderation deutlich verbessert.

Über Einzelfälle hinaus können Jugendorganisationen auch **regelmäßig Zusammenfassungen** von beobachteten Trends einreichen, wie beispielsweise „monatliche Berichte über Online-Gefahren für Jugendliche“ oder „vierteljährliche Trendberichte“. Die

DSCs können diese in ihre jährlichen Risikobewertungen einbeziehen, wodurch sie neue Muster erkennen und Plattformen für das Versäumnis, weit verbreitete Gefahren zu bekämpfen, zur Rechenschaft ziehen können.

Krisenreaktions- und Schnelleskalationsmechanismen

Bestimmte Online-Gefahren eskalieren schnell und erfordern sofortiges Handeln. Dazu gehören beispielsweise virale Suizid-Challenges, koordinierte Hasskampagnen gegen eine Schule, die Verbreitung intimer Bilder von Minderjährigen oder Gewaltdrohungen. In solchen Fällen können die üblichen Meldewege zu langsam sein. Die DSA trägt dem Rechnung und ermöglicht es den DSCs, spezielle Krisenreaktionsverfahren zu aktivieren.

Dafür wird mit dem Digital Security Committee ein Krisenprotokoll erarbeitet . Dieses Protokoll legt fest, wie beide Parteien in Notfällen kommunizieren, welche Informationen die NGO bereitstellen muss, wie das DSC die betreffende Plattform kontaktiert und wie beide Organisationen Folgemaßnahmen koordinieren. Beispielsweise kann die NGO einen vorformatierten Notfallbericht an ein dafür eingerichtetes, rund um die Uhr erreichbares Postfach des DSC senden. Dieser Bericht sollte Details wie Zeitstempel, betroffene Personen (anonymisiert), Screenshots und den Kontext des Vorfalls enthalten. Das DSC kann die Plattform dann umgehend anweisen, Inhalte zu entfernen oder Schutzmaßnahmen zu ergreifen.

Ein klar definiertes Protokoll legt auch fest, wann ein Vorfall über das DSC hinaus eskaliert werden sollte. Hat die Krise grenzüberschreitende Auswirkungen oder betrifft sie eine sehr große Online-Plattform (VLOP), kann das DSC die Europäische Kommission hinzuziehen. In extremen Fällen – wie etwa bei Bedrohungen der öffentlichen Sicherheit – können weitere staatliche Institutionen eingeschaltet werden.

Für Jugendorganisationen verringert ein solches Protokoll die Unsicherheit, beschleunigt die Reaktionszeiten und stärkt das Vertrauen junger Menschen in die verfügbaren Unterstützungsangebote . Allein das Vorhandensein eines klaren Eskalationsverfahrens kann die Situation von Opfern von Online-Schaden deutlich verbessern .

Unterstützung systemischer Risikoanalysen und Forschung

Eine wichtige Neuerung des DSA ist die Verpflichtung für sehr große Online-Plattformen, jährlich **systemische Risikoanalysen durchzuführen** . Diese Analysen untersuchen, wie Plattformdesign, Algorithmen, Geschäftsmodelle und Systeme zur Inhaltsmoderation Risiken, insbesondere für Minderjährige, erzeugen oder verstärken können. Die DSCs (Digital Security Committees) sind für die Prüfung dieser Analysen, die Anforderung zusätzlicher Informationen von den Plattformen und die Bewertung der Angemessenheit der Risikominderungsmaßnahmen zuständig.

Jugendorganisationen können in diesem Prozess eine entscheidende Rolle spielen, indem sie empirische Daten, Beispiele aus der Praxis und Kontextinformationen beisteuern, die

Plattformen oft übersehen. Beispielsweise könnte die Risikobewertung einer Plattform auf Basis automatisierter Moderationsstatistiken behaupten, dass Cybermobbing-Fälle zurückgehen. Jugendarbeiter beobachten jedoch möglicherweise, dass sich das Mobbing lediglich in private Kanäle verlagert oder subtilere Verhaltensmuster entwickelt hat. Solche Erkenntnisse sind für Jugendschutzorganisationen von unschätzbarem Wert, da sie es ihnen ermöglichen, die Behauptungen der Plattformen zu hinterfragen und strengere Schutzmaßnahmen zu fordern.

Zusammenarbeit kann vielfältige Formen annehmen. Jugendorganisationen können an **Fokusgruppen teilnehmen** , sich an **Konsultationen beteiligen, jährliche oder thematische Forschungsergebnisse** teilen oder sich den vom DSC eingerichteten **Arbeitsgruppen anschließen** . Sie können auch mit akademischen Einrichtungen kooperieren, um Daten zu erheben, die DSC-Untersuchungen unterstützen oder politische Empfehlungen beeinflussen. In einigen Ländern finanzieren DSCs sogar zivilgesellschaftliche Monitoring-Initiativen oder vergeben Stipendien für Forschungsprojekte zur Jugendsicherheit.

Durch ihre Beteiligung an systemischen Risikoanalysen tragen Jugendorganisationen dazu bei, dass regulatorische Entscheidungen die gelebten Erfahrungen junger Menschen widerspiegeln und nicht auf abstrakten Annahmen beruhen. Dies stärkt zudem ihre Legitimität als Akteure in der Digitalpolitik und verstärkt ihren Einfluss auf die Sicherheitsstandards, die Plattformen einhalten müssen.

Sensibilisierung, Prävention und öffentliche Kommunikation

Neben der Durchsetzung von Gesetzen sollen DSCs auch Initiativen zur Förderung digitaler Kompetenzen und zur Sensibilisierung der Öffentlichkeit unterstützen. Sie können landesweite Kampagnen durchführen, Informationsmaterialien veröffentlichen oder mit Schulen zusammenarbeiten. Jugendorganisationen sind in diesem Bereich natürliche Partner, da sie bereits im Bildungsbereich tätig sind und enge Verbindungen zu Jugendlichen, Lehrkräften, Eltern und lokalen Gemeinschaften pflegen.

Gemeinsame Aufklärungskampagnen können vielfältig sein. Einige konzentrieren sich darauf, jungen Menschen manipulative Gestaltungstechniken von Plattformen zu vermitteln oder ihnen das Verständnis von Datenschutzeinstellungen zu erleichtern. Andere thematisieren Cybermobbing, die Auswirkungen sozialer Medien auf die psychische Gesundheit oder den verantwortungsvollen Umgang mit Inhalten. Jugendorganisationen tragen mit ihrem praktischen Wissen dazu bei, welche Botschaften bei jungen Menschen Anklang finden und welche Formate – Workshops, Videos, Peer-Education-Aktivitäten – am effektivsten sind.

DSCs können Jugendorganisationen auch bei der Entwicklung von Bildungsmaterialien unterstützen, indem sie regulatorische Rahmenbedingungen, juristische Expertise oder Zugang zu Plattformleitfäden bereitstellen. In einigen Ländern fördern DSCs sogar finanziell NGOs, die Bildungsprogramme entwickeln, die auf die Ziele der DSA abgestimmt sind.

Dadurch entsteht ein Ökosystem, in dem Prävention, Bildung und Strafverfolgung sich gegenseitig verstärken.

Die durch gemeinsame Kampagnen erzielte Sichtbarkeit stärkt zudem die Glaubwürdigkeit von Jugendorganisationen, was ihnen helfen kann, Finanzmittel zu sichern, neue Zielgruppen zu erreichen und ihre Interessenvertretung zu intensivieren.

Datenschutz, Vertrauen und ethische Überlegungen

Jegliche Zusammenarbeit zwischen Jugendorganisationen und Jugendhilfeeinrichtungen muss die Privatsphäre und Würde junger Menschen respektieren. Jugendarbeiter sammeln häufig sensible Informationen, darunter persönliche Daten, Screenshots und Berichte über schädliche Vorfälle. Bei der Weitergabe solcher Informationen an Jugendhilfeeinrichtungen müssen NGOs die Grundsätze der Datenminimierung, Anonymisierung und sicheren Übertragung sorgfältig beachten.

Das bedeutet nicht, dass die Zusammenarbeit schwierig ist. Vielmehr erfordert sie klare interne Richtlinien und Vereinbarungen mit den Aufsichtsbehörden. Viele DSCs entwickeln standardisierte Berichtsvorlagen, um die unnötige Erhebung personenbezogener Daten zu vermeiden. Jugendorganisationen können diese Vorlagen übernehmen und so die Einhaltung der Vorschriften gewährleisten und die betroffenen Personen schützen.

Ethisch gesehen müssen Jugendorganisationen auch abwägen, wann eine Meldung angebracht ist, insbesondere wenn ein junger Mensch zögert, einen Vorfall zu eskalieren. NGOs sollten die Vorteile der Einbeziehung einer Aufsichtsbehörde erläutern, wie beispielsweise eine stärkere Rechenschaftspflicht der Plattformen oder den Zugang zu schnellen Reaktionsmechanismen. Gleichzeitig sollten sie die Autonomie und das emotionale Wohlbefinden des jungen Menschen respektieren. Die Zusammenarbeit mit Jugendhilfeeinrichtungen muss stets die Grundsätze des Jugendschutzes wahren und sicherstellen, dass junge Menschen sichere, respektvolle und stärkende Unterstützung erhalten.

Langfristige Partnerschaft und Kapazitätsaufbau

Eine effektive Zusammenarbeit mit digitalen Sicherheitszentren (DSCs) ist keine einmalige Angelegenheit, sondern eine langfristige Partnerschaft, die sich mit den sich ändernden digitalen Risiken und Plattformpraktiken weiterentwickelt. Um diese Partnerschaft aufrechtzuerhalten, sollten Jugendorganisationen in den Aufbau interner Kapazitäten investieren – beispielsweise durch Schulungen der Mitarbeitenden zu den Verfahren der digitalen Sicherheitsanalyse (DSA), die Aktualisierung der Meldeprotokolle oder die Festlegung klarer Rollen innerhalb der Organisation für die Kommunikation mit dem DSC.

Jugendorganisationen können sich, sofern sie die Kriterien erfüllen, für den Status **eines Trusted Flaggers (vertrauenswürdiger Melder)** gemäß DSA bewerben. Diese Melder werden von den Plattformen prioritär behandelt und pflegen eine formelle Beziehung zum

DSC. Auch Organisationen, die sich nicht bewerben, können einen wertvollen Beitrag zur Durchsetzung der Vorschriften und zur Analyse systemischer Risiken leisten.

Langfristig kann die Zusammenarbeit mit digitalen Sicherheitszentren (DSCs) die Arbeitsweise von Jugendorganisationen grundlegend verändern. Anstatt isoliert zu agieren, werden sie in die nationale Online-Sicherheitspolitik integriert. Ihre Erkenntnisse fließen in Entscheidungen ein, ihre Daten bilden die Grundlage für nationale Risikobewertungen, und ihre Präventionsprogramme ergänzen regulatorische Maßnahmen. So entsteht ein Multi-Stakeholder-Ökosystem, in dem junge Menschen besser geschützt sind, schädliche Inhalte effektiver bekämpft werden und Plattformen für die von ihnen geschaffenen digitalen Umgebungen zur Rechenschaft gezogen werden.

Zusammenfassend lässt sich sagen, dass das Gesetz über digitale Dienste eine neue Ära für Jugendorganisationen einläutet. Durch die strategische Zusammenarbeit mit Koordinatoren für digitale Dienste können NGOs ihre Wirkung verstärken, zu systemischen Veränderungen beitragen und sicherstellen, dass junge Menschen in Europa in Online-Räumen aufwachsen, die ihre Sicherheit, ihre Rechte und ihre Würde respektieren.

Co-funded by the European Union