STIFTUNG DATENSCHUTZ

Datenschutzrechtliche Fragestellungen beim Betrieb einer Fediverse-Instanz – am Beispiel von Mastodon

Wissenschaftlicher Aufsatz

Autorin
Rebecca Sieber

Idee und Projektleitung
Hendrik vom Lehn

Version: 1.1

Dieser Aufsatz erscheint begleitend zur Publikation

Datenschutz bei Mastodon
Leitfaden für den Instanz-Betrieb im dezentralen Netzwerk

Online verfügbar unter
sds-links.de/mastodon-leitfaden

Autorinnen des Leitfadens sind **Jens Kubieziel, Malte Engeler und Rebecca Sieber.**

Datenschutzrechtliche Fragestellungen beim Betrieb einer Fediverse-Instanz – am Beispiel von Mastodon

Inhaltsübersicht

1. Einleitung

1.1 Problemaufriss

Nach der Übernahme von Twitter durch Elon Musk waren die Augen zahlreicher Microbloggerinnen[1] auf Mastodon gerichtet. Auch die Tage von Reddit schienen gezählt, was die Aufmerksamkeit auf Dienste wie Lemmy oder Kbin/Mbin lenkte. Diese Alternativen haben eine Gemeinsamkeit: Sie nutzen das gleiche offene Protokoll namens ActivityPub[2] und sind damit Teil des sogenannten Fediverse. Das Fediverse ist ein freies föderales soziales Netzwerk[3], genauer gesagt, es sind freie Verbünde von sozialen Netzwerken. Die verschiedenen Server oder Instanzen des Fediverse werden nicht von einem einzigen Unternehmen betrieben, sondern von zahlreichen Organisationen, Privatpersonen oder auch staatlichen Institutionen.[4] Finanziert wird der Betrieb einer Instanz meist durch Spenden oder aus der eigenen Tasche.

Die große „Massenwanderung" in das Fediverse, die so manche Instanzbetreiberinnen ins Schwitzen brachte, ist inzwischen abgeebbt. Aber auch die Prophezeiung, dass das Social-Media-Zeitalter zu Ende sei,[5] hat sich nicht erfüllt. Viele sind bei den Plattformen der Tech-Giganten geblieben oder setzen ihre Hoffnung auf neue proprietäre Dienste wie Bluesky.[6] Das Fediverse hingegen muss erst einmal beweisen, dass es wirklich ein besserer Ort ist. Dass das Nutzungsverhalten im Fediverse nicht getrackt wird, führt auch dazu , dass sich die Reichweite schwer messen lässt. Das Bundesministerium für Bildung und Forschung hat deswegen sogar kürzlich den Rückzug aus dem Fediverse erklärt.[7] Dennoch wächst das Fediverse kontinuierlich und bleibt der große Hoffnungsträger der „digitalen Gegenwelt".[8]

---

1 Für eine bessere Lesbarkeit wird in diesem Beitrag das generische Femininum verwendet. Gemeint sind alle Menschen, aber ggf. auch juristische Personen, andere Institutionen oder Organisationen.
2 https://www.w3.org/TR/activitypub/.
3 Vgl. https://hu.berlin/SocialMediaFreedom.
4 Vgl. *Raman* et al., Challenges in the Decentralised Web: The Mastodon Case, IMC '19: Proceedings of the Internet Measurement Conference, New York 2019, https://doi.org/10.1145/3355369.3355572, S. 224.
5 Vgl. *Moorstedt*, Ist das Zeitalter der sozialen Medien vorbei? Netzkolumne in der Süddeutschen Zeitung v. 13.11.2022, https://www.sueddeutsche.de/kultur/social-media-zukunft-essay-1.5695071.
6 Siehe etwa https://mashable.com/article/bluesky-9-million-users-brazil-ban-x.
7 Siehe https://social.bund.de/@bmbf_bund/113079108198680952.
8 *Mey*, Der Kampf um das Internet. Wie Wikipedia, Mastodon und Co. Die Tech-Giganten herausfordern, München 2023, S. 12 ff.

Nicht weniger erwähnenswert als Mastodon sind insbesondere auch Friendica und Pixelfed, die optisch und funktional an Facebook oder Instagram erinnern. Mit Loops soll sogar ein TikTok-"Klon" entstehen.[9] Daneben gibt es umfangreichere Software wie Hubzilla, zahlreiche Misskey-Forks oder die Event-Plattformen Mobilizon und Gancio. Hierbei handelt es sich nur um einen kleinen Ausschnitt aus den „unendlichen Weiten des Fediverse". Viele der Projekte versuchen Twitter, Youtube oder TikTok nicht nur zu kopieren, sondern alternative Wege dabei zu gehen, eine neue und demokratischere Infrastruktur für soziales Netzwerken aufzubauen. Dazu zählen auch Instanzen, die als Kollektiv oder Kooperative organisiert sind.[10]

Das Fediverse verspricht mehr digitale Autonomie und gilt als datenschutzfreundliche Alternative.[11] Anders als zentralisierte und proprietäre Online-Plattformen werden Fediverse-Instanzen meist nicht profitorientiert betrieben. Fediverse-Plattformen nutzen offene Protokolle, sodass trotz unterschiedlicher Software über Instanzen hinweg kommuniziert werden kann. Dadurch, dass es keinen zentralen Knotenpunkt im Fediverse gibt, wird eine effektive Überwachung der Account-Inhaberinnen erschwert. Damit bieten sich beispielsweise auch weniger Geschäftsmodelle an, die auf personalisierter Werbung basieren. Fediverse-Instanzen sind keine „Walled Gardens"; teilweise ist sogar ein Umzug zu einer anderen Instanz möglich.

Die Software steht unter einer freien Lizenz und kann insofern auch auf einem eigenen Server betrieben werden. Das setzt technische Vorkenntnisse voraus, die nicht jede Person mitbringt. Ein großer Teil der Nutzerinnen registriert sich daher eher auf einigen wenigen größeren Instanzen.[12] Dennoch gibt es tausende Instanzen, deren ehrenamtliche Betreiberinnen in die Verlegenheit kommen, sensible Daten von Nutzerinnen aufzubewahren. Erst im Mai 2023 wurde eine unverschlüsselte Backup-Kopie einer Mastodon-Datenbank vom FBI beschlagnahmt, nachdem deren Besitzerin an einer Demonstration teilgenommen hatte.[13] Mit der Aufmerksamkeit, die vor allem Mastodon erhält, nehmen auch die Sorgen darüber zu, welche

9 https://loops.video/.
10 Beispielhaft sei hier die Mastodon-Instanz https://social.coop/ genannt, die von einer Kooperative betrieben wird.
11 Siehe Bescheid des BfDI vom 17.02.2023 zur Untersagung der von der Bundesregierung betriebenen Facebook-Seite, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Dokumente-allg/2023/Bescheid-Facebook-Fanpage.pdf?__blob=publicationFile&v=1.
12 Siehe https://fediverse.observer/list. Nach dem Stand vom 06.09.2024 wurden 16 Fediverse-Instanzen mit je über 100.000 Accounts gezählt.
13 Siehe https://kolektiva.social/@admin/110637031574056150.

juristischen Angriffsflächen der Betrieb einer Fediverse-Instanz bietet.[14] Es stellt sich die Frage, wie datenschutzfreundlich das Fediverse wirklich ist und ob das Fediverse nicht sogar neue datenschutzrechtliche Probleme aufwirft.

Soziale Netzwerke zeichnen sich gerade dadurch aus, dass dort eine Vielzahl von personenbezogenen Daten verarbeitet werden.[15] Insofern existiert auch im Fediverse ein Spannungsfeld zwischen Selbstdarstellung, dem positiven Ausdruck informationeller Selbstbestimmung und der Gefährdung der Rechte und Freiheiten betroffener Personen.[16] Viele Informationen werden in sozialen Netzwerken freiwillig öffentlich geteilt. Dadurch, dass Menschen immer mehr Zeit mit sozialen Medien verbringen, werden insgesamt immer mehr Informationen gespeichert, die potenziell verwertet werden können.[17] Ein Risiko liegt darin, dass zwischenmenschliche Beziehungen offenbart werden. Hinzu kommt, dass Messenger-Funktionen wie die „direkten Beiträge“ teilweise auch für die private Kommunikation genutzt werden. Damit können sogar vertrauliche Informationen in die Hände von Unbefugten gelangen. Vor allem Instanzbetreiberinnen haben Zugriff auf diese Informationen, ebenso auf Bestandsdaten wie E-Mail- und IP-Adressen sowie Antworten auf Umfragen aller Account-Inhaberinnen der Instanz. Auch im Fediverse verbleiben also Risiken für die Rechte und Freiheiten betroffener Personen.

Dass Freie Software von allen genutzt werden kann, bedeutet auch, dass sich eine unerwünschte oder nicht rechtskonforme Nutzung des Fediverse schwer verhindern lässt. Insbesondere die Videosharing-Plattform PeerTube erhielt negative Schlagzeilen, weil Rechtsextreme ihre Inhalte über PeerTube-Instanzen verbreiten. Wie auch die PeerTube-Entwicklerin Framasoft betont, ist die Moderation von Inhalten im Fediverse daher von überragender Wichtigkeit.[18] Instanzbetreiberinnen müssen nicht nur die eigene Instanz moderieren, sondern auch unmoderierte, sogenannte „Free Speech“-Instanzen von der Föderation ausschließen. An dieser Stelle sei auf die Forschungsergebnisse von *Kissane* und

---

14 Vgl. *Kissane/Kazemi*, Findings Report: Governance on Fediverse Microblogging Servers, 2024, https://fediverse-governance.github.io/, S. 111.
15 Dazu *Hornung*, Datenschutzrechtliche Aspekte der Social Media. In: Hornung/Müller-Terpitz (Hrsg.), Rechtshandbuch Social Media, 2. Aufl., Berlin 2021, S. 131 f.
16 Siehe auch *Hornung*, Datenschutzrechtliche Aspekte der Social Media. In: Hornung/Müller-Terpitz (Hrsg.), Rechtshandbuch Social Media, 2. Aufl., Berlin 2021, S. 132.
17 Vgl. *Hornung*, Datenschutzrechtliche Aspekte der Social Media. In: Hornung/Müller-Terpitz (Hrsg.), Rechtshandbuch Social Media, 2. Aufl., Berlin 2021, S. 132.
18 Siehe https://joinpeertube.org/news/isd-study.

Kazemi verwiesen, die die umfangreichen Herausforderungen bei der Governance von Fediverse-Instanzen untersucht haben.[19]

Ein kollektives Projekt wie das Fediverse erfordert auf jeden Fall einen langen Atem. Da es über geringe finanzielle Ressourcen verfügt und vor allem von ehrenamtlichem Engagement lebt, benötigt es mehr Unterstützung durch den Staat und die Zivilgesellschaft. Bisher sind zwar keine Sanktionen gegen Instanzbetreiberinnern bekannt. Das Fediverse verdient aber eine weitergehende rechtswissenschaftliche Diskussion, damit Instanzen rechtskonform und rechtssicher betrieben werden können. Die strukturelle Benachteiligung des Fediverse zeigt sich auch darin, dass neue Produkte der Techgiganten stets umfassend in der juristischen Fachwelt beleuchtet werden, wie beispielsweise das „Metaverse", das sich längst als Hype offenbart hat.[20] Um das Fediverse bleibt es hingegen ziemlich still. Ein Blick auf einschlägige Gesetze und Rechtsprechung macht deutlich, dass das Fediverse bisher nicht mitgedacht wird. Dieser Aufsatz soll einen Beitrag dazu leisten, dass sich das ändert. Er widmet sich den datenschutzrechtlichen Fragestellungen, die sich bei dem Betrieb einer Mastodon-Instanz ergeben, und einiger unmittelbar daran anknüpfender Themen. Es werden vor allem die umstrittenen Fragen mit dazu vertretbaren Ansichten dargestellt und Lösungsansätze für den datenschutzrechtskonformen Instanzbetrieb vorgeschlagen.

1.2 Fokus auf Mastodon als Untersuchungsgegenstand

Der Fokus dieser Untersuchung liegt auf Mastodon, womit allerdings keine Empfehlung für gerade diese Software verbunden ist. Eine datenschutzrechtliche Analyse, die alle Fediverse-Plattformen in den Blick nimmt, würde jedoch Gefahr laufen, oberflächlich und damit weniger hilfreich zu sein. Jede Software bringt Besonderheiten mit sich, die aufgrund der Vielfalt im Fediverse nicht alle in diesem Aufsatz untersucht werden können.

Derzeit ist Mastodon am verbreitetsten, weshalb ein besonderes Interesse an Klärung der datenschutzrechtlichen Fragen in Bezug auf Mastodon besteht. Hinzu kommt, dass das Fediverse stark von Mastodon und dessen Interpretation des ActivityPub-Standards geprägt ist. Je nach Software spielen auch weitere Protokolle eine Rolle. Damit die folgenden Ausführungen

19 *Kissane/Kazemi*, Findings Report: Governance on Fediverse Microblogging Servers, 2024, https://fediverse-governance.github.io/.
20 Siehe https://protos.com/the-metaverse-bubble-has-popped-we-have-charts-to-prove-it/.

nicht zu kompliziert werden, bezieht sich dieser Aufsatz speziell auf den Betrieb einer Mastodon-Instanz. Die Datenverarbeitungsvorgänge der verschiedenen Fediverse-Plattformen, die ActivityPub nutzen, unterscheiden sich zwar nicht wesentlich. Dennoch gibt es deutliche Unterschiede wie die Gestaltung der Webseiten, die mitgelieferten Datenschutzhinweise und die Konfigurationsmöglichkeiten. Zusätzliche rechtliche Anforderungen ergeben sich zum Beispiel auch für Videosharing-Plattformen wie PeerTube.[21] Die Event-Plattform gancio wiederum ist wesentlich datensparsamer gestaltet und bringt andere Fragestellungen mit sich.

Einige der Ausführungen sind dennoch auf andere Mikro- und Makroblogging-Plattformen des Fediverse übertragbar. In dieser Version des Aufsatzes werden deshalb die Begriffe Fediverse und Fediverse-Instanz verwendet, wenn die jeweiligen Ausführungen nicht nur auf Mastodon zutreffen.

1.3 Eingrenzung des Themas auf datenschutzrechtliche Probleme

Dieser Aufsatz befasst sich in erster Linie mit datenschutzrechtlichen Fragestellungen, die sich aus der DSGVO und dem Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) ergeben. Die hier dargestellte Rechtslage bezieht sich auf Instanzbetreiberinnen in Deutschland, die die Instanz in Deutschland ansässigen Account-Inhaberinnen zur Verfügung stellen. Probleme aus anderen Rechtsgebieten werden nur am Rande thematisiert, zum Beispiel Impressumspflichten und Haftungsfragen. Es wird auch in den Blick genommen, inwieweit der DSA zu beachten ist. Hinsichtlich der konkreten Anforderungen kann aber auf die Leitfäden des IFTAS[22] und des Information Law and Policy Lab[23] verwiesen werden. Vertragsrechtliche Fragen im Nutzungsverhältnis werden hier nur soweit berührt wie dies für die Klärung der Rechtsgrundlage für die Datenverarbeitung erforderlich ist. Ausgeklammert ist zum Beispiel auch der Umgang mit Anfragen von Strafverfolgungsbehörden auf Herausgabe von personenbezogenen Daten. Es wird an dieser Stelle jedenfalls dringend davon abgeraten, Daten von Account-Inhaberinnen herauszugeben, ohne dass die auskunftsverlangende Behörde für ihre Anfrage eine Rechtsgrundlage angibt. Aufgrund der hohen Risiken für die Interessen

21 Siehe dazu Sieber, K&R 2022, 50 (53 f.) – Open-Access-Version: https://cloud.weizenbaum-institut.de/s/m2mDDqfXFnJ3w2K.
22 Siehe https://about.iftas.org/2024/04/09/dsa-guide-for-the-fediverse/.
23 Siehe https://ilplab.nl/2024/06/26/the-fediverse-meets-the-dsa/.

betroffener Personen wird auf jeden Fall zu anwaltlicher Beratung in derartigen besonderen Situationen geraten.

1.4 Perspektive der Instanzbetreiberinnen

In diesem Beitrag wird ausschließlich auf die Perspektive von privaten Instanzbetreiberinnen, wie Einzelpersonen, Vereinen oder Unternehmen, eingegangen. Der Betrieb von Mastodon-Instanzen durch staatliche Stellen wirft besondere Fragen auf, die in diesem Beitrag nicht abschließend beantwortet werden. Auch die Verantwortlichkeit anderer Beteiligter wird nur insoweit angesprochen, wie sie beispielsweise für die Frage der gemeinsamen Verantwortlichkeit relevant ist. Ausgeklammert ist auch die Perspektive von (App-)Entwicklerinnen oder Account-Inhaberinnen, wie beispielsweise die Frage, ob Account-Inhaberinnen selbst Anbieterinnen von digitalen Diensten sind.

2. Technische Grundlagen

2.1 Historische Vorbilder

Die Idee dezentraler, verteilter oder „föderaler“ sozialer Netzwerke[24] ist nicht neu. Das Internet an sich ist ein dezentrales System, bestehend aus mehreren sog. autonomen Systemen, in der Regel Internetdienstanbieter. Schon vor Entstehung des WWW etablierte sich das Usenet als dezentral organisiertes Netzwerk von Diskussionsforen. Auch die E-Mail-Technologie, deren Vorläufer sich bis in die 1960er Jahre zurückdatieren lassen, folgt dieser dezentralen Struktur. Einem ähnlichen Prinzip wie das Simple Mail Transfer Protocol (SMTP) folgt auch Jabber, ein 1999 veröffentlichtes Protokoll für dezentrales bzw. föderales Instant Messaging, welches später Extensible Messaging and Presence Protocol (XMPP) genannt wurde.[25]

Mit der zunehmenden Verbreitung des Internets wurde der gesellschaftliche Fokus immer mehr auf das WWW gelegt. Seit Anfang der 2000er Jahre wurde das Usenet langsam von Webforen abgelöst. Gleichzeitig ließ sich ein Trend hin zur Zentralisierung des Internets beobachten, insbesondere durch den Erfolg großer Unternehmen, die sich Netzwerkeffekte zunutze machen. In dieser Phase entstanden auch die ersten sozialen Netzwerke wie MySpace, Facebook und Twitter. Zuerst verwendeten Dienste wie Facebook oder Google Talk noch XMPP, dann wurden sie jedoch immer mehr zu sog. „Walled Gardens“. Aus der FLOSS-Community heraus entstand dazu eine Gegenbewegung, sodass sich ab etwa 2010 dezentrale und föderale soziale Netzwerke ausbreiten.

Eine der ersten bekannten Alternativen ist der Mikroblogging-Dienst identi.ca, anfangs betrieben mit der Software Laconica, welche später in StatusNet und schließlich in GnuSocial umbenannt wird.[26] Laconica verwendete zunächst das OpenMicroBlogging-Protokoll, das später vom OStatus-Standard abgelöst wurde.[27] Der OStatus-Standard beschreibt das Zusammenspiel

---

24 Vgl. https://de.wikipedia.org/wiki/Verteiltes_soziales_Netzwerk.
25 Siehe https://de.wikipedia.org/w/index.php?title=Extensible_Messaging_and_Presence_Protocol&oldid=234321536.
26 Vgl. https://de.wikipedia.org/w/index.php?title=Identi.ca&oldid=228049455; https://de.wikipedia.org/w/index.php?title=GNU_Social&oldid=233533160; https://github.com/fabacab/laconica.
27 Vgl. https://de.wikipedia.org/w/index.php?title=OStatus&oldid=222774690.

mehrerer verbreiteter offener Protokolle, die föderiertes MicroBlogging ermöglichen.[28] Eine wichtige Grundlage dafür bilden insbesondere Atom- und RSS-Feeds,[29] und schließlich ActivityStreams[30]. Später stieg identi.ca auf die effizientere pump.io-Software um, deren Protokolle auch als Vorbild für ActivityPub dienen.[31] Weitere frühe Projekte sind diaspora und Mistpark bzw. Friendica. Dass sich schließlich ActivityPub als Protokoll durchsetzte, dürfte sehr zur Interoperabilität zwischen diesen Diensten beigetragen haben. Ein wichtiger Faktor ist aber auch, dass diese Projekte meist Copyleft-Lizenzen wie die Affero GNU General Public License (AGPL)[32] verwenden. Dadurch können die Entwicklerinnen den Quellcode der anderen Projekte untersuchen und aufeinander aufbauen.

In gewisser Weise parallel zum Fediverse haben sich auch Projekte entwickelt, die soziale Netzwerke auf Basis von XMPP aufbauen wollten.[33] Andere Projekte verfolgen einen Peer2Peer-Ansatz, wie Twister und Secure Scuttlebutt.[34] Diese Ansätze sind interessant und möglicherweise datenschutzfreundlicher, scheinen sich gegenüber ActivityPub aber bis auf Weiteres nicht durchzusetzen.[35]

Für Blockchain-basierte Technologien wird der Begriff der Dezentralisierung ebenfalls verwendet, jedoch eher als Marketing-Buzzword. Derartige machtkonzentrierende Technologien werden in der Fediverse-Community überwiegend abgelehnt. In diesem Zusammenhang ist das web0-Manifesto zu erwähnen, mit dem sich die Fediverse-Community von der Idee des „Web3“ abgrenzt.[36]

---

28 Siehe https://en.wikipedia.org/w/index.php?title=OStatus&oldid=1163781683.
29 Siehe https://www.w3.org/community/ostatus/wiki/The_Basics.
30 https://www.w3.org/TR/activitystreams-core/.
31 Siehe https://en.wikipedia.org/w/index.php?title=Pump.io&oldid=1125130270.
32 https://www.gnu.org/licenses/agpl-3.0.html.
33 Vgl. https://en.wikipedia.org/w/index.php?title=Comparison_of_software_and_protocols_for_distributed_social_networking&oldid=1163579354.
34 Vgl. https://en.wikipedia.org/w/index.php?title=Comparison_of_software_and_protocols_for_distributed_social_networking&oldid=1163579354.
35 Vgl. https://ariadne.space/2019/01/07/activitypub-the-worse-is-better-approach-to-federated-social-networking/.
36 https://web0.small-web.org/.

2.2 Offene Standards

2.2.1 ActivityPub

Auch Mastodon verwendete anfangs den OStatus-Standard, stieg dann aber auf den ActivityPub-Standard um, der seit 2018 von der W3C empfohlen wird.[37] ActivityPub baut wie schon OStatus auf der ActivityStreams-Spezifikation auf, die wie ActivityPub von der Social Web Working Group des W3C erarbeitet wurde.[38] Mit ActivityStreams wird eine Syntax für „Activities" in sozialen Medien beschrieben, unter Verwendung des JSON-Dateiformats.[39] Die verwendeten Begriffe wie *Activity*, *Object*, *Actor* oder *Collection* werden im Activity Vocabulary definiert.[40]

Der ActivityPub-Standard besteht aus zwei Ebenen, und zwar aus der „Social API", dem Client-to-Server-Protokoll, und dem eigentlichen „Federation Protocol", dem Server-to-Server-Protokoll.[41] Allerdings spielt das Client-to-Server-Protokoll nur eine untergeordnete Rolle, da die sogenannte Mastodon API (auch „MastoAPI" genannt) den anderen Projekten gewisse faktische Zwänge auferlegt.[42]

Die Basis für ActivityPub stellen die *Objects* dar, wobei es sich zum Beispiel um *Notes*, also einen Status oder Beitrag, oder um eine *Question*, eine Umfrage handeln kann. Diese werden in einer *Activity* „verpackt", das heißt in einer für soziale Netzwerke typischen Handlung. Eine *Activity* kann das Erstellen oder Löschen eines Beitrags sein, das „Favorisieren" oder „Boosten", sprich das Teilen eines Beitrags oder das Senden einer Folgeanfrage. Die Activities werden stets einem bestimmten *Actor* zugeordnet, womit zum Beispiel ein Account gemeint sein kann, aber auch eine Instanz oder eine Gruppe. Die *Actor* besitzen je eine Inbox und eine Outbox in Gestalt von URLs, über die sie Beiträge auch über Instanzen hinweg erhalten oder versenden können.

---

37 Siehe https://de.wikipedia.org/w/index.php?title=ActivityPub&oldid=235047239.
38 Siehe https://www.w3.org/TR/activitypub/; https://www.w3.org/TR/activitystreams-core/.
39 Siehe https://www.w3.org/TR/activitystreams-core/.
40 Siehe https://www.w3.org/TR/activitystreams-vocabulary/.
41 Siehe https://www.w3.org/TR/activitypub/.
42 Vgl. https://flak.tedunangst.com/post/ActivityPub-as-it-has-been-understood.

Sendet die Account-Inhaberin Alice beispielsweise einen direkten Beitrag an Account-Inhaber Bob, „postet“ sie diese zunächst in ihre eigene Outbox. Der Server von Alice verpackt die Nachricht in eine *Create Activity* und sendet diese an die Inbox von Bob. Bob kann anschließend die Nachricht von seiner Inbox abrufen. Diesem Prinzip nach würde ein öffentlich geposteter Beitrag von Alice's Outbox an die Inboxes aller Actor gesendet werden, die Alice folgen. Um diese Verteilung effizienter zu gestalten, teilen sich die Actor einer Instanz eine Inbox, die *Shared Inbox*. Nach dem ActivityPub-Standard werden also alle öffentlich gepostete Beiträge nicht direkt an die Inboxes aller folgenden Actor versendet, sondern an die Shared Inboxes aller Instanzen, auf denen ein Actor dem Actor A folgt. Die sog. föderierte Timeline einer Fediverse-Instanz setzt sich grundsätzlich aus eben dieser Shared Inbox zusammen.

2.2.2 „MastoAPI“

Mastodon weicht nicht nur wesentlich vom Client-to-Server-Protokoll von ActivityPub ab,[43] sondern ergänzt die W3C-Empfehlung insgesamt in einiger Hinsicht.[44] Für Betreiberinnen anderer Fediverse-Instanzen, die mit anderer Software betrieben werden, genügt es daher nicht der W3C-Empfehlung zu folgen. Damit diese auch mit Mastodon-Instanzen „sprechen“ können, müssen diese sich auch an der „MastoAPI“ orientieren.[45]

Der ActivityPub-Standard schlägt insbesondere noch keinen bestimmten Mechanismus für die Authentifizierung und Autorisierung vor.[46] Mastodon verwendet HTTP-Signaturen, um zu verifizieren, dass eine Activity tatsächlich von einem bestimmten Actor stammt.[47] Auf Client-to-Server-Ebene kommt auch der OAuth-Standard zum Einsatz, um den Client gegenüber dem Server zu autorisieren.[48]

Mastodon verwendet außerdem WebFinger, das nicht Teil von ActivityPub ist, aber auch vom OStatus-Standard erfasst wird.[49] WebFinger wird in diesem Fall dazu verwendet, anhand eines

---

43 Siehe https://activitypub.rocks/implementation-report/.
44 Vgl. https://blog.soykaf.com/post/activity-pub-in-pleroma/, zitiert nach https://flak.tedunangst.com/post/ActivityPub-as-it-has-been-understood.
45 Vgl. https://blog.soykaf.com/post/activity-pub-in-pleroma/, zitiert nach https://flak.tedunangst.com/post/ActivityPub-as-it-has-been-understood.
46 Siehe https://www.w3.org/TR/activitypub/#authorization.
47 Siehe https://docs.joinmastodon.org/spec/security/.
48 Siehe https://docs.joinmastodon.org/methods/oauth/.
49 Siehe https://docs.joinmastodon.org/spec/webfinger/; Vgl. https://en.wikipedia.org/w/index.php?title=OStatus&oldid=1163781683.

Fediverse-Handles nach dem Schema @actor@instanz.de Informationen zu diesem Actor zu ermitteln. Es wird von Mastodon und anderen Fediverse-Instanzen dazu verwendet, den Handle eines Actors in einen HTTP URI zu übersetzen, in diesem Fall in die URL https://instanz.org/users/actor/. Mithilfe von WebFinger kann auch in der Benutzeroberfläche bei Mastodon nach anderen Accounts gesucht werden. Das Alt-Right-Netzwerk Gab verwendet ebenfalls WebFinger, auch wenn es nicht (mehr) mit dem Fediverse föderiert.[50] Daher ist es grundsätzlich möglich, in der Suchmaschine anhand von Handles nach Accounts auf Gab zu suchen und alte Beiträge zu finden.

Bei Mastodon gibt es noch einige weitere Funktionen, zum Beispiel eine Filterfunktion, um unerwünschte Inhalte auszublenden.[51]

2.3 Föderation und Deföderation bei Mastodon

Eine Mastodon-Instanz empfängt alle Beiträge von Account-Inhaberinnen, denen eine Account-Inhaberin der eigenen Instanz folgt. Umgekehrt übermittelt sie die Beiträge der Account-Inhaberinnen an alle Instanzen, auf denen sich eine Followerin dieser Account-Inhaberin befindet. Darüber hinaus können auch sog. Relays eingebunden werden, mit denen Instanzen „unbekannten" Instanzen oder Hashtags folgen können.[52]

Anders funktioniert die Föderation, wenn der *Limited Federation Mode* aktiviert ist, der allerdings den *Secure Mode* (auch *Authorized Fetch*) voraussetzt.[53] Im *Limited Federation Mode* müssen andere Instanzen erst ausdrücklich bestätigt werden, bevor diese die Inhalte der Instanz abrufen können.

Auch die sogenannte Deföderation, das Blocken von Instanzen durch Instanzbetreiberinnen, ist von der W3C-Empfehlung nicht erfasst.[54] Die weichere Variante stellt das „Stummschalten" dar, bei dem die Inhalte der stummgeschalteten Instanzen nicht mehr in der föderierten Timeline

---

50 Danke an *@tobias@social.diekershoff.de* für diesen Hinweis.
51 Siehe https://docs.joinmastodon.org/user/moderating/.
52 Siehe zum Beispiel https://relay.fedimins.net/.
53 Siehe https://docs.joinmastodon.org/admin/config/ und https://docs.joinmastodon.org/spec/activitypub/#secure-mode.
54 Vgl. https://docs.joinmastodon.org/spec/activitypub/#Block und https://www.w3.org/TR/activitypub/#block-activity-outbox.

auftauchen.[55] Beim Blocken einer Instanz werden gar keine Inhalte mehr an diese Instanz übermittelt. Das wird bei Mastodon dadurch realisiert, dass Accounts dieser Instanzen automatisch aus Follower- und Follows-Sammlungen entfernt werden und die HTTP-Signatur des geblockten Servers nicht mehr akzeptiert wird.[56] Allerdings verwendet Mastodon als Default-Einstellung (noch) Linked Data-Signaturen.[57] Werden auf diese Weise Beiträge durch Teilen weitergereicht, kann die Authentifizierung und Autorisierung umgangen werden. Ein effektiveres Blocken ist möglich, sofern der *Secure Mode* oder *Authorized Fetch* aktiviert ist. In diesem Fall sind HTTP-Signaturen sogar für das Abrufen einer Outbox erforderlich.[58] Wenn sich die geblockte Account-Inhaberin auf einer anderen Instanz befindet oder ausgeloggt ist, kann sie aber weiterhin öffentliche Beiträge auf der öffentlichen Seite des Accounts einsehen. Sofern die Einstellung DISALLOW_UNAUTHENTICATED_API_ACCESS durch die Instanzbetreiberin aktiviert wurde, ist auch das nicht mehr möglich.[59]

2.4 Verarbeitungsvorgänge auf Mastodon-Instanzen

Die wesentliche Funktion einer Mastodon-Instanz besteht darin, dass Account-Inhaberinnen sich mit anderen Fediverse-Accounts verbinden, Inhalte teilen und mit anderen interagieren. Im Folgenden wird genauer beschrieben, welche Datenverarbeitungsvorgänge oder Verarbeitungsreihen zu welchen Zwecken stattfinden.

2.4.1 Besuch der Webseite einer Mastodon-Instanz

2.4.1.1 HTTP-Anfrage

Bereits bei dem Besuch einer Fediverse-Instanz werden bestimmte personenbezogene Daten verarbeitet. Das geschieht auch, wenn die betroffene Person selbst keinen Account im Fediverse besitzt, sondern lediglich die Startseite der Instanz, ein Accountprofil oder die URL zu einem bestimmten Beitrag aufruft.

---

55 Vgl. https://docs.joinmastodon.org/methods/accounts/#mute.
56 Vgl. https://docs.joinmastodon.org/methods/admin/domain_blocks/.
57 Siehe https://docs.joinmastodon.org/spec/security/#ld.
58 Siehe https://docs.joinmastodon.org/spec/security/#http.
59 Vgl. https://docs.joinmastodon.org/admin/config/#disallow_unauthenticated_api_access; danke an @Curator@mastodon.art für den Hinweis.

Bei dem Aufruf der Webseite werden zwingend bestimmte Daten auf dem Server verarbeitet, damit die Webseite der Besucherin überhaupt angezeigt werden kann.[60] Vereinfacht kann dies wie folgt beschrieben werden. Gibt eine Besucherin eine Internetadresse in die URL-Leiste des Browsers ein, sendet der Browser eine HTTP-Anfrage an den Server, der diese Webseite hostet. Um diese Anfrage ausführen zu können, benötigt der Server zunächst die eingegebene URL sowie die IP-Adresse, an die der Inhalt der Webseite übermittelt werden soll. Auch der Zeitpunkt des Zugriffs ist ein Datum, das bei diesem Vorgang notwendigerweise verarbeitet wird.

In der Regel sendet der Browser oder die App im Header der Anfrage, dem sog. User-Agent, weitere Daten mit, um die Webseite korrekt und komfortabel darzustellen. Zu diesen Daten gehören beispielsweise Informationen über den verwendeten Browser oder die verwendete App, das Betriebssystem, die Prozessorarchitektur und die im Browser eingestellte Sprache.[61]

Instanzbetreiberinnen können einstellen, wie lange der Server derartige Log-Dateien speichert.[62]

Eine Verbindung der Account-Inhaberin zu einem anderen Server als der Heiminstanz wird nur aufgebaut, wenn beispielsweise die URL des Originalbeitrags aufgerufen wird. Beim Lesen von Beiträgen auf der Heiminstanz werden also nicht die oben beschriebenen, beim Aufruf einer Webseite verarbeiteten, Daten übermittelt.

2.4.1.2 Cookies, Local Storage und Session Storage

In älteren Mastodon-Versionen (z. B. v4.1.3) wurde bei jedem Besuch einer Instanz ein Cookie namens _mastodon_session über den Webbrowser im Speicher der Besucherinnen abgelegt. Es handelte sich hierbei um ein „Rails Session Cookie“, das zusammen mit dem Cookie _session_id dazu diente, die Session und den Status des Login-Prozesses zu speichern (z. B. bei einer Zwei-Faktor-Authentifizierung).[63] Zudem leitete das Cookie die Account-Inhaberin nach dem Login auf die letzte besuchte Seite.[64] In neueren Versionen wird das Cookie erst abgelegt, wenn die Registrierungs- oder Login-Seite aufgerufen wird.

---

60 Vgl. https://developer.mozilla.org/en-US/docs/Web/HTTP.
61 https://de.wikipedia.org/w/index.php?title=User_Agent&oldid=214516660.
62 Vgl. BGH, Urteil vom 16. Mai 2017 – VI ZR 135/13 –, BGHZ 215, 55-69.
63 Siehe https://github.com/mastodon/mastodon/issues/1181.
64 Siehe https://github.com/mastodon/mastodon/issues/23843,

2.4.1.3 Abruf von eingebundenen Medien

Eine Besonderheit bei Mastodon stellt das Einbinden von Medien, insbesondere von Videos, dar. Wenn Account-Inhaberinnen Links auf Video-Hostingdienste wie YouTube oder auch auf PeerTube-Instanzen teilen, werden diese im Beitrag in einem sog. iFrame eingebettet.[65] Auch Account-Inhaberinnen, die nicht eingeloggt sind, können die in öffentlichen Beiträgen eingebetteten Videos sehen. Dabei wird zunächst nur ein Vorschaubild angezeigt, die sog. Preview-Card, die im lokalen Cache der Mastodon-Instanz gespeichert wird. Abgespielt wird das Video erst nach einem Klick auf das Vorschaubild. Der Unterschied zu einer einfachen Verlinkung besteht also zum einen darin, dass der Link nicht nur als URL, sondern mit einem Vorschaubild des Videos angezeigt wird. Die aufgerufene Webseite mit dem Video wird zudem nicht in einem neuen Browserfenster oder -tab geöffnet, sondern direkt in der ursprünglichen Webseite eingebunden.

2.4.2 Registrierungsprozess

Da sich auf Mastodon-Instanzen regelmäßig Spam-Accounts registrieren, ist eine offene Instanz nicht empfehlenswert. In der Community werden bestimmte Maßnahmen gegen Spam diskutiert, beispielsweise ein Spam-Schutz via Captcha oder eine Verifikation mittels Telefonnummer.[66] Diese Maßnahmen würden weitere datenschutzrechtliche Fragen nach sich ziehen, die hier nicht behandelt werden.

Bei geschlossenen Instanzen ist es in der Regel möglich, eine Registrierungsanfrage zu stellen. In vielen Fällen sind dem Registrierungsformular die Nutzungsregeln vorgeschaltet. Sofern diesen zugestimmt wird, wird im nächsten Schritt ein Anzeigename abgefragt, als Pflichtangaben weiterhin ein Account-Name, eine E-Mail-Adresse, ein Passwort und gegebenenfalls ein Grund für den Registrierungswunsch. Unterhalb des Formulars und oberhalb des Buttons „Get on waitlist“ gibt es eine Checkbox, mit der bestätigt wird, dass die Datenschutzhinweise gelesen wurden und akzeptiert werden. Ohne das Bestätigen dieser Checkbox ist eine Registrierung nicht möglich. Anschließend wird ein Bestätigungslink an die angegebene E-Mail-Adresse gesendet, um diese zu verifizieren.

---

65 Siehe https://docs.joinmastodon.org/entities/PreviewCard/#video

66 Vgl. nur https://github.com/mastodon/mastodon/issues/877; https://github.com/mastodon/mastodon/issues/7601.

Diese Bestandsdaten sind für Instanzbetreiberinnen sowohl über die Weboberfläche des Administrations- als auch den Moderationszugang einsehbar. Diese Informationen werden aber, abgesehen vom Anzeigename, nicht mit anderen Instanzen geteilt.[67]

2.4.3 Weitere Profileinstellungen

Wird die Registrierung bestätigt, ist es möglich, den Anzeigenamen zu ändern und weitere Profilinformationen hinzuzufügen, wie eine Biografie, ein Profilbild und ein Headerbild. Diese Daten werden an alle bekannten Instanzen übermittelt, das heißt an alle Instanzen, auf denen ein Account einem Account der eigenen Instanz folgt

Es gibt einige Einstellungen, die die Privatsphäre betreffen und standardmäßig deaktiviert sind. In der Standardeinstellung ist der *Social graph* öffentlich einsehbar, das heißt die Liste aller Followerinnen und Follows ist öffentlich zugänglich. Auch die Indexierung durch Suchmaschinen wird zunächst erlaubt. „Per default" werden auch Folgeanfragen automatisch bestätigt und Beiträge für alle sichtbar veröffentlicht.

2.4.4 Login-Prozess

2.4.4.1 Cookies, Local Storage und Session Storage

Nach dem Login auf der Instanz wird im Speicher der Account-Inhaberin ein weiteres Cookie abgelegt, die sog. _session_id. Dieses Cookie dient zusammen mit der _mastodon_session dazu, die Account-Inhaberin wiederzuerkennen, sodass sich diese nicht bei jedem Besuch der Webseite neu einloggen muss (siehe unter 2.4.1).

2.4.4.2 Nutzungsdaten

In der Weboberfläche des Adminstration- und Moderationszugangs können Instanzbetreiberinnen zudem den Zeitpunkt des letzten Log-ins und die letzten verwendeten IP-Adressen einsehen. Auch die eingestellte Sprache für das Interface wird dort angezeigt.

67 Vgl. https://blog.joinmastodon.org/2023/07/what-to-know-about-threads/.

2.4.5 Interaktion auf der Instanz

2.4.5.1 Folgen und Gefolgtwerden

Das Folgen und Gefolgtwerden von Account-Inhaberinnen richtet sich im Wesentlichen nach der W3C-Empfehlung.[68] Sendet eine Account-Inhaberin eine Folgeanfrage an einen Account, sendet der Server eine *Follow Activity* an die Inbox auf dem Server des Accounts, dem gefolgt werden soll. Je nach Einstellung dieses Accounts wird entweder automatisch eine *Accept Activity* zurückgesendet oder erst dann, wenn die andere Account-Inhaberin die Folgeanfrage akzeptiert hat. Wird die Folgeanfrage abgelehnt, sendet der Server eine *Reject Activity* zurück. Die „Follower" und „Follows" werden jeweils in einer *Collection* zusammengefasst.

2.4.5.2 Erstellen von Beiträgen

Erstellt eine Account-Inhaberin einen neuen Beitrag, wird dieser in der Datenbank des Servers gespeichert und als *Create Activity* zumindest an alle Instanzen gesendet, auf denen jemand dieser Account-Inhaberin folgt. Wie dieser Beitrag veröffentlicht wird und an welche Instanzen der Beitrag übermittelt wird, hängt davon ab, welche Sichtbarkeit die Account-Inhaberin für diesen Beitrag eingestellt hat. Nach der Veröffentlichung kann diese Einstellung nicht geändert werden. Die Account-Inhaberin kann lediglich den Beitrag löschen und mit einer anderen Sichtbarkeitseinstellung neu veröffentlichen.

Das Sichtbarkeitskonzept von Mastodon unterscheidet sich etwas vom ActivityPub-Standard. In der Standardeinstellung werden Beiträge auf Mastodon öffentlich zugänglich gemacht. Diese Beiträge sind dann für alle öffentlich auf der Webseite des Accounts einsehbar, sofern nicht die Einstellung DISALLOW_UNAUTHENTICATED_API_ACCESS durch die Instanzbetreiberin aktiviert wurde.[69] Öffentliche Beiträge werden vom Server an die Sammlung *as:public* adressiert und somit an alle Instanzen übermittelt, auf denen mindestens ein Account der Account-Inhaberin folgt.[70] Auf diesen anderen Instanzen wird anschließend eine Kopie des Beitrags abgelegt. Beiträge können auch nur an die eigenen Followerinnen gesendet werden. Diese „follower-only" veröffentlichten Beiträge sind nicht auf der öffentlichen Webseite zugänglich.

---

68 Vgl. https://docs.joinmastodon.org/spec/activitypub/#supported-activities-for-profiles; https://blog.joinmastodon.org/2018/07/how-to-make-friends-and-verify-requests/.

69 Vgl. https://docs.joinmastodon.org/admin/config/#disallow_unauthenticated_api_access; danke an @Curator@mastodon.art für den Hinweis.

70 Siehe https://docs.joinmastodon.org/spec/activitypub/#Mention.

Diese Beiträge werden nur Followerinnen zugänglich gemacht.[71] Direkte Beiträge werden nur an die Instanzen von Accounts übermittelt, die im Beitrag erwähnt werden, und sind nur für diese Accounts zugänglich.[72] Mastodon ergänzt die Sichtbarkeitseinstellungen von ActivityPub um „ungelistete Beiträge". Diese sind zwar öffentlich auf der Webseite des Accounts sichtbar, werden jedoch nicht auf der föderierten oder der lokalen Timeline angezeigt.[73]

Eine Ende-zu-Ende-Verschlüsselung der direkten Beiträge ist vom ActivityPub-Standard nicht vorgesehen und auch von Mastodon (noch) nicht umgesetzt.[74] Das bedeutet, dass Instanzbetreiberinnen Zugriff auf alle Inhalts- und Metadaten der Accounts auf der Instanz haben.

Bei der Frage des Zugriff auf diese Daten muss unterschieden werden, ob die Instanz selbst auf einem eigenen oder angemieteten (virtuellen) Server betrieben wird oder ein „Managed-Hosting"-Angebot in Anspruch genommen wird. Bei letzterem hat lediglich die Anbieterin des Hosting-Angebots den Zugriff auf direkte Beiträge, da die Administratorin keinen direkten Zugriff auf die Datenbank hat.

2.4.5.3 Löschen von Beiträgen

Beim Löschen eines Beitrags wird dieser aus der Datenbank der Instanz entfernt. Zugleich wird eine „Delete Activity" an alle bekannten Instanzen gesendet, sodass der Beitrag in der Regel auch auf allen anderen Datenbanken gelöscht wird.[75] Es gibt jedoch keine Möglichkeit, absolut sicherzustellen, dass die anderen Instanzen eine solche Löschanfrage auch tatsächlich umsetzen. Insbesondere im Zusammenspiel zwischen verschiedener Fediverse-Software kommt es in diesem Bereich häufig zu Problemen, sodass beispielsweise auf Mobilizon oder Pixelfed gelöschte Beiträge in föderierenden Mastodon-Instanzen weiter sichtbar sein können.[76]

2.4.5.4 Favorisieren und Boosten von Beiträgen

Beim Favorisieren oder Boosten eines Beitrags erstellt der Server eine „Like" bzw. „Announce" Activity, die an alle föderierenden Instanzen übermittelt wird.[77] Diese Informationen sind auf der

71 Siehe https://docs.joinmastodon.org/spec/activitypub/#Mention.
72 Siehe https://docs.joinmastodon.org/spec/activitypub/#Mention.
73 Siehe https://docs.joinmastodon.org/spec/activitypub/#Mention.
74 Vgl. https://github.com/mastodon/mastodon/pull/13820.
75 Vgl. https://docs.joinmastodon.org/spec/activitypub/#status.
76 Vgl. nur https://github.com/Automattic/wordpress-activitypub/issues/16.
77 Siehe https://docs.joinmastodon.org/spec/activitypub/#status.

Webseite des Originalbeitrags öffentlich einsehbar. Wird lediglich eine Kopie auf einem föderierenden Server abgerufen, wird dort nur ein Teil dieser „Likes“ oder „Boosts“ angezeigt. Mittels „Boosten“ eines Beitrags wird der Beitrag auch an alle Account-Inhaberinnen übermittelt, die dem boostenden Account folgen. Auf diese Weise wird der Empfängerkreis öffentlicher Beiträge erweitert.

2.4.5.5 Abstimmen bei Umfragen

Die Account-Inhaberinnen können ihre Beiträge auch mit einer Umfrage verbinden. Sie können dazu bis zu vier Antwortoptionen anhängen und die gewünschte Dauer der Umfrage festlegen. Je nach Einstellung können andere Account-Inhaberinnen anschließend eine oder mehrere der Antworten auswählen und abstimmen. Deren Server speichern dann über ein User-Token, welche Option sie ausgewählt haben.[78] Wenn die so authorisierten Account-Inhaberinnen die Umfrage aufrufen, prüft ihr Server anhand des User-Tokens, ob sie schon abgestimmt haben.[79] Wenn das der Fall ist, zeigt der Server ihnen die Umfrage an und hebt dabei die jeweils ausgewählte(n) Antwortoption(en) besonders hervor.

2.4.5.6 Blocken und stummschalten

Auch Account-Inhaberinnen können andere Instanzen oder Accounts „stummschalten“ oder „blocken“.[80] Schaltet eine Account-Inhaberin einen anderen Account stumm, werden nur für die Stummschaltende die Beiträge des stummgeschalteten Accounts nicht mehr angezeigt.[81] Beim Blocken wird dieser Account gegebenenfalls von der Liste der Followerinnen und der „Follows“ entfernt. Zudem werden Beiträge des geblockten Accounts nicht mehr angezeigt, und auch deren Inhaberin kann die Beiträge der anderen in der Regel nicht mehr über die eigene Instanz einsehen.

2.4.5.7 Melden von Beiträgen

Account-Inhaberinnen können andere Account-Inhaberinnen melden. In einem nächsten Schritt können sie einen Grund für die Meldung auswählen und Beiträge auswählen, die die Meldung bekräftigen sollen. Instanzbetreiberinnen haben dann die Möglichkeit, über das Administrationsmenü Maßnahmen zu ergreifen oder gegebenenfalls auch weitere Beiträge zu

---

78 Vgl. https://docs.joinmastodon.org/entities/Poll/#own_votes.
79 Siehe https://docs.joinmastodon.org/entities/Poll/#voted.
80 Vgl. https://docs.joinmastodon.org/spec/activitypub/#Block und https://www.w3.org/TR/activitypub/#block-activity-outbox.
81 Siehe https://docs.joinmastodon.org/user/moderating/#mute.

melden. Unter anderem können sie die gemeldeten Beiträge löschen oder den jeweiligen Account sperren, was nur innerhalb von 30 Tagen rückgängig gemacht werden kann. Es stehen aber auch mildere Maßnahmen zur Verfügung, wie das „Stummschalten“. Zudem können alle Medienanhänge des Accounts mit einer Inhaltswarnung versehen werden.

3. Grundrechtliche Bezüge

3.1 Unmittelbare Grundrechtsbindung staatlicher Institutionen

Grundrechte richten sich in erster Linie an den Staat, schützen also zunächst vor dem staatlichen Zugriff auf Social-Media-Daten.[82] Auch staatliche Institutionen, die eine Fediverse-Instanz betreiben, sind direkt an Grundrechte gebunden.[83] Das betrifft zum Beispiel die Instanz „social.bund.de“, die aktuell noch von der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) betrieben wird. Deutsche Behörden sind unmittelbar aus dem Grundgesetz dazu verpflichtet, das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG zu beachten. Bürgerinnen können sich auf diesen Instanzen zwar nicht registrieren, sondern jeweils nur Bundesbehörden oder Institutionen der EU. Trotzdem sind auf diesen Instanzen auch personenbezogene Daten von Account-Inhaberinnen anderer Instanzen gespeichert. Wenn beispielsweise eine Social-Media-Beauftragte einer staatlichen Institution Beiträge von Account-Inhaberinnen anderer Instanzen liest, werden diese abgerufen und in der Datenbank der Instanz gespeichert. Derartige Datenverarbeitungen im Rahmen der Nutzung dürften jedenfalls durch die Informationspflicht des Staates im Wege der Öffentlichkeitsarbeit gerechtfertigt sein. In diesem Kontext sollten Inhaberinnen staatlicher Accounts beispielsweise prüfen, ob es möglicherweise geboten ist zu verbergen, welche Accounts ihnen folgen.

Jeder Betrieb eines staatlichen Social-Media-Auftritts stellt einen Eingriff in Grundrechte dar, der verfassungsrechtlich zu rechtfertigen ist.[84] Der Betrieb einer eigenen Mastodon-Instanz ist als relativ milder Eingriff anzusehen. Einer genaueren Prüfung bedarf es hingegen, wenn sich Behörden auf Fediverse-Instanzen von Privatpersonen oder Unternehmen registrieren. Staatliche Account-Inhaberinnen sollten sich in diesem Fall zumindest ausreichende Einflussmöglichkeiten auf Instanzbetreiberinnen vorbehalten, etwa im Wege eines Auftragsverarbeitungsvertrags. Für private Instanzbetreiberinnen bedeutet dies zusätzlichen

82 Dazu *Hornung*, Datenschutzrechtliche Aspekte der Social Media. In: Hornung/Müller-Terpitz (Hrsg.), Rechtshandbuch Social Media, 2. Aufl., Berlin 2021, S. 133 f., 137.
83 Art. 1 Abs. 3 GG.
84 Siehe dazu auch *Engeler*, MMR 2017, 651.

Arbeitsaufwand, sodass davon abzuraten ist, staatliche Accounts auf privaten Instanzen zu dulden.

3.2 Mittelbare Drittwirkung der Grundrechte

Im Verhältnis zwischen Privaten wirken sich Grundrechte eher indirekt aus. Die Grundrechte sind vor allem bei der Auslegung der einschlägigen Gesetze zu berücksichtigen.[85] Schließlich sind auch die Gerichte bei der Anwendung des Rechts an Grundrechte gebunden.[86] Zum Teil verpflichten der DSA und die DSGVO auch Private dazu, Grundrechte unmittelbar zu beachten.[87] Da insoweit EU-Recht angewendet wird, wird das deutsche Grundgesetz von der Grundrechte-Charta der EU überlagert.[88] Im Bereich des Datenschutzes ist vor allem das Recht auf Schutz personenbezogener Daten aus Art. 8 GrCh und das Recht auf Achtung des Privat- und Familienlebens aus Art. 7 GrCh relevant. Ebenso ist die Freiheit der Meinungsäußerung und die Informationsfreiheit aus Art. 11 Abs. 1 GrCh zu beachten. Instanzbetreiberinnen sind insbesondere auch von der Informationsfreiheit geschützt. Es gehört aber auch zu ihrem Grundrecht auf Achtung ihrer Kommunikation, selbst eine Fediverse-Instanz betreiben zu können.

Außerdem kommt dem Staat auch eine Schutzpflicht zu. Sowohl die BRD als auch die EU haben insofern eine Pflicht, durch gesetzliche Regelungen für einen angemessenen Schutz des Grundrechts auf Datenschutz zu sorgen.[89] Der Staat soll aber auch Anreize für die Verbreitung datenschutzfreundlicher Technologien schaffen. Aus rechtspolitischer Sicht ist der Staat daher gefordert, Alternativen wie das Fediverse zu privilegieren und von unverhältnismäßigen Pflichten auszunehmen.

---

85 Vgl. BVerfG, Beschl. v. 11.04.2018 – 1 BvR 3080/09, NJW 2018, 1667 (1668).
86 Vgl. BVerfG, Beschl. v. 11.04.2018 – 1 BvR 3080/09, NJW 2018, 1667 (1668).
87 Siehe z.B. Art. 14 Abs. 4 DSA sowie Art. 6 Abs. 1 f) DSGVO.
88 *Hornung*, Datenschutzrechtliche Aspekte der Social Media. In: Hornung/Müller-Terpitz (Hrsg.), Rechtshandbuch Social Media, 2. Aufl., Berlin 2021, S. 133.
89 *Hornung*, Datenschutzrechtliche Aspekte der Social Media. In: Hornung/Müller-Terpitz (Hrsg.), Rechtshandbuch Social Media, 2. Aufl., Berlin 2021, S. 137 f.

4. Einordnung als digitaler Dienst

Angesichts der Besonderheiten des Fediverse stellt sich die Frage, wie das Fediverse und insbesondere der Betrieb einer Mastodon-Instanz in die rechtlichen Kategorien eingeordnet werden kann. Eine zentrale Frage ist, ob Fediverse-Instanzen als „digitale Dienste“ anzusehen sind. Davon hängt insbesondere ab, ob der neue DSA Anwendung findet. Der DSA enthält einen abgestuften Pflichtenkatalog für Anbieterinnen von Vermittlungsdiensten, sieht für diese aber auch Haftungsprivilegien vor. Auch das neue Digitale-Dienste-Gesetz (DDG), das das Telemediengesetz (TMG) abgelöst hat, knüpft nunmehr an den Begriff des „digitalen Dienstes“ an. Da § 2 Abs. 1 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) auf die Begriffsbestimmungen des DDG verweist, ist diese Einordnung auch maßgeblich dafür, ob und welche datenschutzrechtlichen Sonderregelungen zu beachten sind.

4.1 Dienst der Informationsgesellschaft

Sowohl der DSA als auch das DDG greifen den Begriff des „Dienstes der Informationsgesellschaft“ auf, der auf die Richtlinie über den elektronischen Geschäftsverkehr (E-Commerce-Richtlinie)[90] zurückgeht. Unter einem „Dienst der Informationsgesellschaft“ wird „jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung“ verstanden.[91]

Auf Fediverse-Instanzen scheint dieser Begriff nicht richtig zu passen. Der Begriff der „Dienstleistung“ scheint auch vorauszusetzen, dass zwischen Instanzbetreiberin und Account-Inhaberin ein Vertrag geschlossen wird. Das wiederum setzt voraus, dass sich beide überhaupt rechtlich binden wollen. Das ist insofern zweifelhaft, als dass Fediverse-Instanzen meist ehrenamtlich betrieben werden (siehe dazu die Ausführungen unter 7.2.3). Zweifel können auch daran bestehen, dass Fediverse-Instanzen in der Regel gegen Entgelt angeboten werden. Schließlich bieten die allermeisten Betreiberinnen von Fediverse-Instanzen eine kostenlose

90 RL 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt.

91 Art. 3 a) DSA i.V.m. Art. 1 b) der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft.

Registrierung an. Es sind bisher auch keine Mastodon-Instanzen bekannt, die sich über Werbung finanzieren oder die Account-Inhaberinnen mit ihren Daten „bezahlen“ lassen. Bei den meistgenutzten sozialen Netzwerken wie TikTok oder Instagram sieht das hingegen schon anders aus. Am Beispiel von Threads und Bluesky zeigt sich, dass das Fediverse mittlerweile auch von Anbieterinnen proprietärer Dienste entdeckt wird. Aus der Sicht von „durchschnittlichen“ Verbraucherinnen spielt es keine Rolle, welche Software jeweils im Hintergrund eingesetzt wird. Für viele ist „Mastodon“ ein Ersatz für Twitter, also im Grunde auch nur ein weiteres „soziales Netzwerk“. Nach der hier vertretenen Auffassung kommt es deshalb nicht darauf an, ob Mastodon-Instanzen in der Regel gegen Entgelt angeboten werden. Es sind vielmehr alle vergleichbaren, auch proprietäre soziale Netzwerke in den Blick zu nehmen.[92]

Eine andere Ansicht hierzu vertreten *John/Müller/Rennert*.[93] Ihrer Ansicht nach seien die Betreiberinnen von Mastodon-Instanzen keine Anbieterinnen von Diensten der Informationsgesellschaft, weil es in der Regel an der Entgeltlichkeit fehle. Ihrem Argument, dass unentgeltliche Dienste privilegiert werden sollen, ist an sich zuzustimmen.[94] Die Ansicht der Autorinnen lässt aber unberücksichtigt, dass der Begriff des Dienstes der Informationsgesellschaft auch eingeführt wurde, um für diese einen sicheren Rechtsrahmen zu schaffen. *John/Müller/Rennert* nahmen noch an, dass es sich bei Mastodon-Instanzen um Telemedien handelt, für die das Haftungsprivileg in § 10 TMG galt.[95] Tatsächlich wurde der im alten TMG verwendete Begriff des Telemediums weiter verstanden als sein europäisches Äquivalent.[96] Dieses divergierende Verständnis war jedoch spätestens seit Inkrafttreten des DSA fragwürdig und ist inzwischen ganz hinfällig geworden. Mit dem DDG hat der deutsche Gesetzgeber eine ganz klare Abkehr vom national geprägten Begriff der „Telemedien“ zum Ausdruck gebracht.[97] Im neuen § 7 Abs. 1 DDG wird zwar klargestellt, dass die Haftungsprivilegien in Art. 4-8 DSA auch dann gelten, wenn für die Nutzung eines Dienstes kein Entgelt erhoben wird. Trotzdem sind die Haftungsprivilegien jetzt auch nach deutschem Recht nur für Diensteanbieter vorgesehen. Spätestens seit der Einführung des TDDDG und des DDG lässt sich die Argumentation von *John/Müller/Rennert* schwer aufrecht erhalten.

---

92 Siehe auch *Sieber*, K&R 2022, 50 (53) – Open-Access-Version: https://cloud.weizenbaum-institut.de/s/m2mDDqfXFnJ3w2K.
93 So *John/Müller/Rennert*, GRUR 2023, 691 (697).
94 Vgl. *John/Müller/Rennert*, GRUR 2023, 691 (697).
95 Siehe *John/Müller/Rennert*, GRUR 2023, 691 (694).
96 Dies bejaht *Spindler* in Spindler/Schmitz, Telemediengesetz, 2. Aufl. 2018, § 1 TMG Rn. 6.
97 BT-Drs. 20/10031, S. 67.

Die Diskussion zeigt, dass für Betreiberinnen von Fediverse-Instanzen eine erhebliche Rechtsunsicherheit besteht. Zum einen ist weiterhin unklar, welche Pflichten für sie gelten. Zum anderen stehen sie vor der offenen Frage, ob sie für sämtliche Rechtsverletzungen Dritter haften, oder nur wenn sie nach Kenntnis nicht zügig tätig werden.[98] Es spricht jedoch einiges dafür, Fediverse-Instanzen als Dienste der Informationsgesellschaft einzuordnen. Der Begriff soll schließlich einen sehr weiten Bereich von wirtschaftlichen Tätigkeiten erfassen.[99] Auch gemeinnützige Vereine können wirtschaftlich tätig werden.[100] Eine Gewinnerzielungsabsicht ist hierfür gerade nicht erforderlich.[101] Weder ein Vertrag noch eine monetäre Gegenleistung ist notwendig.[102] Es kommt bei der Frage der Entgeltlichkeit auch nicht darauf an, dass die Dienstleistung von der Person bezahlt wird, der diese zugute kommt.[103] Auch der Betrieb einer Mastodon-Instanz muss auf irgendeine Weise bezahlt oder querfinanziert werden, beispielsweise durch Spenden. Im Erwägungsgrund 18 der E-Commerce-Richtlinie werden beispielhaft auch solche Dienste genannt, „die Informationen, die von einem Nutzer des Dienstes stammen, speichern".[104] Jedenfalls aus Sicht von Verbraucherinnen dürften solche Instanzen, auf denen sich auch andere Personen als die Betreiberinnen registrieren können, auch im Fediverse die Regel darstellen.

Es kann deshalb davon ausgegangen werden, dass es sich bei Fediverse-Instanzen um „Dienste der Informationsgesellschaft" handelt. Instanzbetreiberinnen haften somit nur dann für Rechtsverletzungen von Dritten, wenn sie nicht unverzüglich nach Kenntnis tätig werden (Art. 6 Abs. 1DSA). Die aus dieser Einordnung resultierenden Pflichten für Instanzbetreiberinnen sind überschaubar, wie die folgenden Abschnitte zeigen sollen.

98 Siehe dazu auch Spindler, CR 2023, 602 (603).
99 Siehe Erwägungsgrund 18 der E-Commerce-Richtlinie; *Hofmann,* in: Hofmann/Raue (Hrsg.) Digital Services Act, 1. Aufl. 2023, Art. 3 Rn. 6.
100 Siehe EuGH, Urt. v. 19.6.2014, EuZW 2014, 672.
101 Siehe EuGH, Urt. v. 19.6.2014, EuZW 2014, 672.
102 Vgl. Erwägungsgrund 18 der E-Commerce-Richtlinie.
103 Vgl. EuGH, Urt. v. 26.4.1988 – C-352/85.
104 Siehe Erwägungsgrund 18 der E-Commerce-Richtlinie.

4.2 Digital Services Act

Der DSA scheint den „Dienst der Informationsgesellschaft“ als Oberbegriff für bestimmte Arten von Diensten zu verwenden.[105] Die verschiedenen Arten von Diensten und die jeweils einschlägigen Vorschriften werden im Folgenden näher beleuchtet.

4.2.1 Vermittlungsdienst

Der Anwendungsbereich des DSA erstreckt sich lediglich auf Vermittlungsdienste.[106] Diese erfassen allerdings ein sehr weites Spektrum von Diensten. Dazu zählen zum einen „Hosting“-Dienste, welche darin bestehen, von einem Nutzer bereitgestellte Informationen in dessen Auftrag zu speichern.[107] Aber auch interpersonelle Telekommunikationsdienste können Vermittlungsdienste sein.[108] Im DSA wird klargestellt, dass Diensteanbieterinnen auch verschiedene Arten von Vermittlungsdiensten gleichzeitig erbringen können.[109] Die Anwendbarkeit weiterer Vorschriften des DSA muss insofern immer bezogen auf die konkrete technische Funktion geprüft werden.[110] Nur wenn einzelne Dienste nicht voneinander abgegrenzt werden können, kommt es auf den Schwerpunkt des Dienstes an.[111]

Auf Fediverse-Instanzen sind jedenfalls die allgemeinen Vorschriften für Vermittlungsdienste anwendbar. Instanzbetreiberinnen sind daher insbesondere verpflichtet, eine zentrale Kontaktstelle für Behörden und Nutzerinnen zu benennen (Art. 11 und 12 DSA). Sie dürfen auch nicht willkürlich die Account-Inhaberinnen auf ihrer Instanz sperren oder deren Beiträge löschen, sondern müssen etwaige Nutzungsregeln in den AGB transparent machen (Art. 14 DSA).

Art. 15 DSA verpflichtet die Anbieterinnen von Vermittlungsdiensten darüber hinaus, mindestens einmal jährlich einen Transparenzbericht zur Verfügung zu stellen. „Kleinst- und Kleinunternehmen“ sind von dieser Pficht ausgenommen.[112] Damit sind „Unternehmen“ gemeint, die weniger als 50 Personen beschäftigen und deren Jahresumsatz bzw. Jahresbilanz 2

105 Vgl. *Hofmann*, in: Hofmann/Raue (Hrsg.) Digital Services Act, 1. Aufl. 2023, Art. 3 Rn. 5.
106 Art. 2 Abs. 2 DSA.
107 Vgl. Art. 3 g) iii) DSA.
108 Erwägungsgrund 29; so auch im Umkehrschluss aus Erwägungsgrund 14 des DSA.
109 Siehe Erwägungsgrund 15, 29 des DSA.
110 Siehe Erwägungsgrund 29 des DSA.
111 Siehe auch Köhler, in: Müller-Terpitz/Köhler (Hrsg.), DSA, 1. Aufl. 2024, Art. 3, Rn. 10.
112 Art. 15 Abs. 2 DSA.

Millionen Euro nicht übersteigt.[113] Instanzbetreiberinnen stehen damit vor der Frage, ob die Ausnahme auch für sie gilt, wenn sie eine Instanz als Privatperson betreiben. In Art. 3 f) DSA wird der „Unternehmer" definiert als jede natürliche oder juristische Person, unabhängig davon, ob sie in privatem oder öffentlichem Eigentum steht, die für die Zwecke ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit entweder selbst oder durch eine andere in ihrem Namen oder Auftrag handelnde Person tätig wird. Der Betrieb der Fediverse-Instanz kann zumindest in einigen Fällen bereits als geschäftliche Tätigkeit angesehen werden. Der Begriff der Unternehmerin ist weit zu verstehen.[114] Jedenfalls gebietet es die Gleichheit vor dem Gesetz, dass auch Fediverse-Instanzen von diesen weitergehenden Pflichten auszunehmen sind, sofern sie nicht von Unternehmen betrieben werden. Hinter der Ausnahme steht schließlich der Gedanke, dass unverhältnismäßige Belastungen für kleine Unternehmen vermieden werden sollen.[115] Der Grund dafür wird darin gesehen, dass diese über weniger finanzielle und personelle Ressourcen verfügen und zugleich ein geringeres Gefahrenpotenzial aufweisen.[116] Diese Überlegungen treffen erst recht auf Privatpersonen und gemeinnützige Organisationen zu.[117]

4.2.2 Hosting-Dienst

Fediverse-Instanzen können jedenfalls als Hostingdienste angesehen werden, soweit sie von einem Nutzer bereitgestellte Informationen speichern. Die jeweiligen Vorschriften gelten damit vor allem dann, wenn Instanzbetreiberinnen Registrierungen anderer Personen zulassen. Weniger eindeutig ist dies bei „Ein-Personen-Instanzen". Letztendlich speichern jedoch auch diese die Beiträge von Account-Inhaberinnen anderer Instanzen.

Art. 16 DSA schreibt für Hosting-Dieste ein Melde- und Abhilfeverfahren vor. Instanzbetreiberinnen müssen die eingegangenen Meldungen zeitnah, objektiv und sorgfältig bearbeiten.[118] Ein Problem bei Mastodon könnte darin bestehen, dass nur Account-Inhaberinnen Inhalte über die Meldefunktion melden können. Zudem fehlen bei der Meldefunktion einige

113 Art. 19 Abs. 1 DSA i.V.m. Art. 2 Abs. 2 und 3 der Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, K(2003) 1422, ABl. L 124 vom 20.5.2003, S. 36–41.
114 *Köhler*, in: Müller-Terpitz/Köhler (Hrsg.), DSA, 1. Aufl. 2024, Art. 3, Rn. 40, 42.
115 *Köhler*, in: Müller-Terpitz/Köhler (Hrsg.), DSA, 1. Aufl. 2024, Art. 19, Rn. 1.
116 *Raue*, in: Hofmann/Raue (Hrsg.) Digital Services Act, 1. Aufl. 2023, Art. 19 Rn. 1.
117 So im Ergebnis auch *Wiedemann*, GRUR-Prax 2023, 411.
118 Art. 16 Abs. 6 DSA.

vorgesehene Elemente, wie die Angabe einer E-Mail-Adresse. Insofern ist fraglich, ob die Ausgestaltung des Meldeverfahrens den Anforderungen des Art. 16 Abs. 2 DSA genügt. Sofern die Inhalte auch per E-Mail an Instanzbetreiberinnen gemeldet werden können, ist jedoch davon auszugehen, dass das Meldeverfahren ausreichend benutzerfreundlich ausgestaltet ist.[119]

Wenn Instanzbetreiberinnen Beiträge „ihrer" Account-Inhaberinnen löschen oder deren Accounts sperren, müssen sie dies gegenüber den Account-Inhaberinnen verständlich begründen und bestimmte Angaben hierzu machen.[120] Eine Befreiung von dieser Pflicht ist beispielsweise bei der Löschung von „Spam" oder der Sperrung von „Fake-Accounts" anzunehmen.[121]

Außerdem verpflichtet Art. 18 DSA Instanzbetreiberinnen dazu, sich gegebenenfalls bei den Strafverfolgungs- oder Justizbehörden zu melden. Diese Pflicht besteht, wenn Instanzbetreiberinnen Kenntnis von Informationen erhalten, die den Verdacht einer bestimmten Straftat begründen. Davon sind jedoch nicht alle Straftaten erfasst, sondern nur solche, die eine Gefahr für das Leben oder die Sicherheit einer Person oder von Personen darstellen.

4.2.3 Online-Plattform

Der DSA enthält zusätzliche Vorschriften für Online-Plattformen und beschreibt diese als Hosting-Dienste, die Informationen nicht nur im Auftrag einer Nutzerin speichern, sondern auch öffentlich verbreiten.[122] Die „öffentliche Verbreitung" meint die Bereitstellung von Informationen für eine potenziell unbegrenzte Zahl von Personen.[123] An einer öffentlichen Verbreitung fehlt es beispielsweise dann, wenn andere Personen erst in einer Nutzerinnengruppe aufgenommen werden müssen, um Zugang zu den Informationen erhalten.[124] Auf Beiträge, die nur für Followerinnen sichtbar sind, dürften die Vorschriften für Online-Plattformen daher nicht anwendbar sein.

---

119 Vgl. *Raue*, in: Hofmann/Raue (Hrsg.) Digital Services Act, 1. Aufl. 2023, Art. 16 Rn. 31.
120 Art. 17 Abs. 1 DSA.
121 Art. 17 Abs. 2 Uabs. 2 DSA; vgl. *Raue*, in: Hofmann/Raue (Hrsg.) Digital Services Act, 1. Aufl. 2023, Art. 17 Rn. 35, 37.
122 Art. 3 f) DSA; Erwägungsgrund 13 des DSA.
123 Erwägungsgrund 14 des DSA.
124 Erwägungsgrund 14 des DSA.

Auch interpersonelle Kommunikationsdienste, wie beispielsweise E-Mail oder Instant-Messaging-Dienste, sollen nicht vom Begriff der Online-Plattform erfasst sein.[125] Ob die Funktion der „direkten Beiträge“, die nur für erwähnte Personen sichtbar sind, einen interpersonellen Kommunikationsdienst darstellt, wird unter 5.2 näher erläutert. An dieser Stelle kann diese Frage offen bleiben, weil es hinsichtlich der direkten Beiträge jedenfalls an einer öffentlichen Verbreitung der Inhalte fehlt.

Soweit Beiträge öffentlich sichtbar verbreitet werden, kann eine Mastodon-Instanz zweifellos als Online-Plattform eingeordnet werden. Gemäß Art. 3 i) DSA darf es sich dabei nicht um eine unbedeutende und reine Nebenfunktion eines anderen Dienstes handeln, die aus objektiven und technischen Gründen nicht ohne diesen anderen Dienst genutzt werden kann. Der Kommentarbereich einer Online-Zeitung soll insofern nicht als Online-Plattform angesehen werden – die Speicherung von Kommentaren in einem sozialen Netzwerk hingegen schon.[126] Trotz verschiedener Sichtbarkeitseinstellungen dürfte es sich bei den „öffentlichen Beiträgen“ nicht lediglich um eine Nebenfunktion handelt. Das sogenannte „Micro-Blogging“ stellt vielmehr einen wesentlichen Bestandteil von Mastodon dar, der zumindest eine gleich bedeutsame Rolle spielt wie „direkte Beiträge“ oder „follower-only Beiträge“.

Im Ergebnis können die Vorschriften für Online-Plattformen von Instanzbetreiberinnen dennoch vernachlässigt werden, da die allermeisten dieser Vorschriften nicht für Kleinst- und Kleinunternehmen gelten.[127] Es kann insofern auf die Ausführungen unter 4.2.1 verwiesen werden. Instanzbetreiberinnen müssen lediglich den Aufsichtsbehörden auf Verlangen die durchschnittliche monatliche Zahl ihrer aktiven Nutzerinnen aus der EU nennen.[128] Problematisch hieran ist, dass die Information, ob Account-Inhaberinnen in der EU leben, gar nicht erhoben wird. Bislang dürfte es sich hierbei aber eher um ein theoretisches Problem handeln.

125 Erwägungsgrund 14 des DSA.
126 Siehe Erwägungsgrund 13 des DSA.
127 Art. 19 Abs. 1 DSA.
128 Artt. 19 Abs. 1 S. 1 und Art. 24 Abs. 3 DSA.

4.2.4 Sehr große Online-Plattform

Den „sehr großen Online-Plattformen“ legt der DSA in den Art. 33-43 DSA weitergehende Pflichten auf. Auch die Ausnahmen für Klein- und Kleinstunternehmen gelten nicht, wenn es sich bei dem Dienst um eine sehr große Online-Plattform handelt.[129] Es handelt sich jedoch nur dann um eine sehr große Online-Plattform, wenn diese eine durchschnittliche monatliche Zahl von 45 Millionen aktiven Nutzerinnen in der Union haben und sie von der EU-Kommission als sehr große Online-Plattform benannt worden sind.[130] Bisher hat die EU-Kommission keine Fediverse-Instanz als sehr große Online-Plattform eingeordnet.[131] Selbst große Instanzen wie mastodon.social sind noch weit von dieser Nutzerinnenzahl entfernt. Es kommt schließlich allein darauf an, wie viele Nutzerinnen die einzelne Instanz hat, und nicht auf die Gesamtzahl der Nutzerinnen des Fediverse, die auf etwa 10 Millionen Nutzerinnen geschätzt wird.[132]

4.3 Digitale-Dienste-Gesetz

Das neue DDG schafft den nationalen Rechtsrahmen für Behörden, damit diese den DSA auch in Deutschland umsetzen können. Zugleich löst das DDG das TMG und das Netzwerkdurchsetzungsgesetz (NetzDG) ab. Der noch im alten TMG verwendete Begriff des „Telemediums“ hat damit ausgedient. Daher fallen einige schwierige Fragen weg, beispielsweise die Frage, ob der Anwendungsbereich der nationalen Regelungen im TMG über den des DSA hinausging (siehe 4.1). Der „digitale Dienst“ wird schließlich in § 1 Abs. 4 DDG mit dem „Dienst der Informationsgesellschaft“ gleichgesetzt. Das DDG gilt für alle Anbieterinnen von digitalen Diensten, mit Ausnahme von Rundfunkanbieterinnen.[133]

Das DDG verweist nun auf die Haftungsprivilegien im DSA. Der Hinweis in § 7 Abs. 1 DDG, dass die Haftungsprivilegien unabhängig davon gelten, ob für die Nutzung des Dienstes ein Entgelt erhoben wird, dürfte hingegen keine eigenständige Bedeutung haben. Wie unter 4.1 erläutert wurde, kommt es nicht darauf an, ob ein konkreter Dienst ein Entgelt erhebt, sondern nur darauf, dass der Dienst „in der Regel“ gegen Entgelt angeboten wird.

---

129 Siehe Art. 15 Abs. 2 DSA und Art. 19 Abs. 2 DSA.
130 Art. 33 Abs. 1, Abs. 4 DSA.
131 Vgl. https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413.
132 Vgl. https://mastodon.fediverse.observer/stats.
133 § 1 Abs. 1 S. 1, 3, Abs. 4 Nr. 5 DDG.

Wie das alte TMG regelt auch das DDG eine sogenannte „Impressumspflicht“. Damit wird Art. 5 der E-Commerce-Richtlinie in das nationale Recht überführt. Die Impressumspflicht ist nunmehr in § 5 DDG geregelt und weist keine Unterschiede zur Vorgängerregelung auf. Wie auch nach dem alten TMG kann das Fehlen eines Impressums ein Bußgeld nach sich ziehen.[134] Die konkreten Anforderungen an das Impressum und ein Musterbeispiel finden sich im Leitfaden unter „Praktische Umsetzung und notwendige Musterdokumente“.

134 § 33 Abs. 2 Nr. 1, Abs. 6 Nr. 3 DDG.

5. Adressatinnen datenschutzrechtlicher Pflichten

Mit Blick auf die datenschutzrechtlichen Pflichten kann die Frage aufgeworfen werden, ob diese überhaupt an Betreiberinnen von Fediverse-Instanzen adressiert sind.

Zum einen stellt sich die Frage, ob die besonderen Vorschriften des TDDDG zu beachten sind, welche sich jeweils teilweise an Anbieterinnen von digitalen Diensten und teilweise an Anbieterinnen von Telekommunikationsdiensten richten. Das TDDDG ist aber nur dann vorrangig gegenüber der DSGVO zu beachten, soweit mit dem TDDDG die Regelungen der EU-Richtlinie 2002/58/EG für elektronische Kommunikation (E-Privacy-RL) umgesetzt werden.[135]

Zum anderen stellt sich die wichtige Vorfrage, ob und inwieweit Instanzbetreiberinnen überhaupt „Verantwortliche" im Sinne der DSGVO sind oder die Daten als „Auftragsverarbeiterinnen" im Auftrag der Account-Inhaberinnen verarbeiten. Aufgrund der vielen beteiligten Personen im Fediverse ist außerdem zu klären, ob möglicherweise mehrere Personen „gemeinsam verantwortlich" sind und somit eine Vereinbarung über die gemeinsamen Pflichten nach Art. 26 DSGVO treffen müssen.

5.1 Anbieterinnen von digitalen Diensten

Teil 3 des TDDDG enthält einige Regelungen zum Datenschutz bei digitalen Diensten. Hervorzuheben ist hier vor allem die sogenannte „Cookie Banner"-Regelung in den §§ 25, 26 TDDDG.

Im Übrigen ist fraglich, welche Bedeutung die Regelungen des TDDDG zum Datenschutz bei digitalen Diensten haben. Die weiteren Vorschriften zum Datenschutz bei digitalen Diensten können dann relevant werden, wenn die DSGVO aufgrund der „Haushaltsausnahme" in Art. 2 Abs. 1 c) DSGVO nicht anwendbar ist oder keine personenbezogenen Daten betroffen sind.[136]

135 Art. 95 DSGVO.
136 Siehe *Eckhardt/Lepperhoff*, in: Schwartmann/Jaspers/Eckhardt (Hrsg.), TTDSG, 1. Aufl. 2022, § 19 Rn. 11 f.

Ob Account-Inhaberinnen ebenfalls als Anbieterinnen von digitalen Diensten anzusehen sind, wird an dieser Stelle ausgeklammert.

5.2 Anbieterinnen von Interpersonellen Kommunikationsdiensten

Das TDDDG enthält auch Regelungen zum Datenschutz und zum Schutz der Privatsphäre in der Kommunikation. Für Betreiberinnen von Fediverse-Instanzen stellt sich insbesondere die Frage, ob Beiträge, die nur für Followerinnen oder erwähnte Personen sichtbar sind, dem Fernmeldegeheimnis unterliegen.

Die Pflicht zur Wahrung des Fernmeldegeheimnisses richtet sich unter anderem an Anbieterinnen von öffentlich zugänglichen Telekommunikationsdiensten.[137] Diese unterliegen auch einem umfangreichen Pflichtenkatalog aus dem Telekommunikationsgesetz (TKG), der für ehrenamtlich betriebene Fediverse-Instanzen nur schwer zu überblicken und umzusetzen sein dürfte. Insbesondere sind die Anbieterinnen von öffentlich zugänglichen Telekommunikationsdiensten verpflichtet, Überwachungsmaßnahmen umzusetzen und Auskünfte über Bestands- und Verkehrsdaten an Strafverfolgungs- und Polizeibehörden zu erteilen.[138] Hinzu kommen unter anderem Pflichtangaben zum Vertragsschluss, die in downloadbarer Form erfolgen sollen, und die Benennung eines Sicherheitsbeauftragten.[139]

5.2.1 Interpersoneller Telekommunikationsdienst

Mit dem Europäischen Kodex für Elektronische Kommunikation (EKEK)[140] wurde der Begriff des Telekommunikationsdiensts um den Begriff des interpersonellen Kommunikationsdiensts erweitert. Das TDDDG verweist insofern auf den Begriff des interpersonellen Kommunikationsdienstes im Telekommunikationsgesetz (TKG).[141] Demnach kommt es darauf an, dass eine interpersonelle und interaktive Kommunikation zwischen einer endlichen Zahl von Personen ermöglicht wird und die Empfängerinnen jeweils bestimmt werden.[142] Hingegen handelt es sich nicht um einen interpersonellen Kommunikationsdienst, wenn es sich dabei um

137 § 3 Abs. 2 Nr. 1 TDDDG.
138 §§ 170, 174 TKG.
139 §§ 54 f., 166 TKG:
140 Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11.12.2018 über den europäischen Kodex für die elektronische Kommunikation.
141 §§ 2 Abs. 1 TTDSG, § 3 Nr. 24, 40, 61 TKG.
142 § 3 Nr. 24 TKG.

eine unbedeutende und untrennbar mit einem anderen Dienst verbundene Nebenfunktion handelt.[143] Mit der Erweiterung auf interpersonelle Kommunikationsdienste sollten insbesondere Messenger-, aber auch E-Mail-Dienste erfasst werden.[144] Dahinter stand der Gedanke, dass diese sich aus der Perspektive der Endnutzerinnen nicht von „klassischen" Telekommunikationsdiensten unterscheiden.[145] Soziale Netzwerke sollten hingegen nicht darunter fallen, wobei hiermit vermutlich vor allem das öffentliche Verbreiten von Beiträgen gemeint war.[146]

Der Bundesbeaufragte für Datenschutz und Informationsfreiheit (BfDI) hat sich an der Konsultationsphase zum Leitfaden beteiligt und – als insoweit zuständige Aufsichtsbehörde – empfohlen, die Funktion der direkten Beiträge und „follower only"-Beiträge nicht als Telekommunikationsdienste anzusehen.[147] Die Argumentation überzeugt in Hinblick auf „follower only"-Beiträge, weil es hier tatsächlich an einem interaktivem Informationsaustausch fehlen dürfte. Die Empfängerinnen werden zwar von den Personen bestimmt, die die Telekommunikation veranlassen oder daran beteiligt sind.[148] Die Beiträge und Antworten hierauf werden aber jeweils nur einseitig den eigenen Followerinnen zugänglich gemacht. Die Beiträge der Account-Inhaberinnen sind immer nur für den eigenen Adressatinnenkreis sichtbar. Somit findet die Kommunikation nicht in einer geschlossenen Gruppe statt, wie es bei den in Erwägungsgrund 17 EKEK genannten Gruppenchats der Fall ist. Es handelt sich vielmehr um eine Privatsphäreneinstellung, die vor dem Hintergrund des in Art. 25 DSGVO normierten „privacy by design" auch erforderlich sein dürfte.

Bei „direkten Beiträgen" dürfte hingegen schon von einem interaktiven Informationsaustausch auszugehen sein. Der BfDI erklärte hierzu, dass es sich lediglich um eine untrennbar mit einem anderen Dienst verbundene untergeordnete Nebenfunktion handle.[149] Die Funktion könne aus objektiv technischen Gründen nicht ohne den Hauptdienst genutzt werden und unterscheide sich auch anwenderinnenseitig nicht von der allgemeinen Beitragsfunktion. Dem ist insofern zuzustimmen, als dass die verschiedenen Funktionen und Sichtbarkeitseinstellungen untrennbar

143 Art. 2 Nr. 5 EKEK; Piltz/Quiel, CR 2022, 263 (264).
144 Siehe *Piltz/Quiel*, CR 2022, 263.
145 Siehe Erwägungsgrund 15 EKEK.
146 Siehe Erwägungsgrund 17 EKEK.
147 Siehe https://sds-links.de/mastodon-konsultation-bfdi.
148 Vgl. § 3 Nr. 24 TKG.
149 Siehe https://sds-links.de/mastodon-konsultation-bfdi.

miteinander verbunden sind.[150] Hierbei ist weniger die Erkennbarkeit für Nutzerinnen entscheidend, als vielmehr die technische Funktionsweise.[151] Entscheidend ist, dass die MastoAPI keine eigene Nachrichtenfunktion vorsieht, sondern Beiträge lediglich mit einer eingeschränkten Sichtbarkeit „veröffentlicht" werden. Sie werden zudem über die gleiche Weboberfläche abgerufen und landen in der gleichen „Timeline". Dem könnte allerdings auch entgegen gehalten werden, dass das Menü von Mastodon auch eine Übersicht über alle privaten Erwähnungen enthält. Rein technisch wäre es auch denkbar, eine Mastodon-App zu entwickeln, die ausschließlich Beiträge anzeigt, in denen die Account-Inhaberinnen privat erwähnt werden.

Weniger überzeugend ist jedenfalls die Annahme, dass die Funktion der „direkten Beiträge" eine unbedeutende reine Nebenfunktion sei. Dieses Merkmal ist aus der objektiven Sicht der Account-Inhaberinnen zu beurteilen und ist als Ausnahmetatbestand eng auszulegen.[152] Von einer unbedeutenden Nebenfunktion kann nur ausgegangen werden, wenn die Funktion für Account-Inhaberinnen einen sehr begrenzten Nutzen hat und von diesen kaum genutzt wird.[153] Als Beispiel hierfür werden Kommunikationskanäle bei Online-Spielen genannt.[154] Die im Fediverse versendeten „direkten Beiträge" sind damit schwer vergleichbar. Die Hauptfunktion von Mastodon dürfte zwar in dem „Microblogging"-Dienst bestehen, der es ermöglicht, Beiträge öffentlich sichtbar zu machen. Das allein lässt jedoch nicht den Schluss zu, dass die Nebenfunktion der „direkten Beiträge" völlig unbedeutend wäre. Schließlich wird diese Funktion durchaus für die private Kommunikation genutzt.

Tatsächlich wird Mastodon im allgemeinen Sprachgebrauch nicht als „Messenger" bezeichnet, anders als die föderalen Instant Messenger, die beispielsweise XMPP oder das Matrix-Protokoll nutzen. Zweifelhaft ist jedoch, ob es in dieser Frage auf das jeweils genutzte Protokoll oder auf das Layout der verwendeten Software ankommen kann. Beispielsweise ähneln Friendica oder Pixelfed ihrem äußeren Erscheinungsbild nach den Diensten Facebook und Instagram, deren Messenger-Funktionen ebenfalls als interpersonelle Kommunikationsdienste zu qualifizieren sind. Dort werden die „direkten Beiträge" auch nicht wie bei Mastodon als „private Erwähnungen", sondern als „(Direkt-)Nachrichten" bezeichnet.

---

150 So auch *John/Müller/Rennert*, GRUR 2023, 691 (698).
151 Siehe Erwägungsgrund 17; *Piltz/Quiel*, CR 2022, 263 (267).
152 Siehe Erwägungsgrund 17; *Piltz/Quiel*, CR 2022, 263 (267).
153 Siehe Erwägungsgrund 17.
154 Siehe Erwägungsgrund 17.

Eine gewisse Rolle spielt zwar auch, wie die Funktion „beworben“ wird.[155] Die Startseite einer Mastodon-Instanz enthält die föderierte Timeline der Instanz, also alle bekannten öffentlichen Beiträge. Dass es auch möglich ist, direkte Beiträge zu versenden, wird lediglich in den von Mastodon mitgelieferten Datenschutzhinweisen beschrieben. Auch auf der Startseite der Mastodon gGmbH ist diese Funktion nicht erwähnt.[156] Beim Verfassen eines direkten Beitrags wird eine Warnung eingeblendet, dass direkte Beiträge nicht Ende-zu-Ende-verschlüsselt sind. Es wird ausdrücklich davon abgeraten, sensible Informationen über Mastodon zu teilen. Eine Ende-zu-Ende-Verschlüsselung ist aber auch bei klassischen Telekommunikationsdiensten nicht vorgesehen, sodass die technische Funktionsweise für Endnutzerinnen insofern keinen spürbaren Unterschied ausmacht.

Gegen die Geltung des Fernmeldegeheimnisses für soziale Netzwerke wird teilweise eingewandt, dass es Instanzbetreiberinnen erlaubt sein sollte, diese Inhalte zu überwachen, um Account-Inhaberinnen vor Spam, Mobbing oder Betrug zu beschützen.[157] Eine solche paternalistische Interpretation ist jedoch bedenklich, weil damit das Fernmeldegeheimnis praktisch ausgehebelt werden würde.

Zusammenfassend lässt sich festhalten, dass es gute Gründe sowohl dafür als auch dagegen gibt, Mastodon-Instanzen als interpersonelle Kommunikationsdienste anzusehen. Entgegen der Ansicht des BfDI erscheint es nach hiesiger Auffassung jedoch konsequent, jedenfalls die Funktion der „direkten Beiträge“ als interpersonellen Kommunikationsdienst einzuordnen.

5.2.2 Öffentlich zugänglich

Die Pflichten aus dem TKG dürften dennoch in aller Regel nicht gelten. Es kann schließlich bezweifelt werden, dass es sich bei Fediverse-Instanzen um „öffentlich zugängliche“ Telekommunikationsdienste handelt. Das wäre dann der Fall, wenn die Instanz einem unbestimmten Personenkreis zur Verfügung steht (§ 3 Nr. 44 TKG). Selbst bei Instanzen mit offener Registrierung ist fraglich, ob diese einem völlig beliebigen und unbegrenzten Personenkreis zugänglich sein sollen.[158] In der Regel behalten sich Instanzbetreiberinnen vor, Personen zu sperren, deren Werte nicht in Einklang mit der jeweiligen Community stehen.

155 Siehe *Piltz/Quiel*, CR 2022, 263 (267).
156 https://joinmastodon.org/.
157 So *Assion*, in: Assion (Hrsg.), TTDSG, 1. Aufl. 2022, § 3 TTDSG Rn. 87.

Fediverse-Instanzen streben zudem kein unbegrenztes Wachstum an und können jeweils nur eine begrenzte Anzahl von Account-Inhaberinnen aufnehmen. Hinter dieser Einschränkung auf öffentlich zugängliche Dienste stand der Gedanke, der Verhältnismäßigkeit Rechnung zu tragen. Kleinere Kommunikationsdienste sollten von aufwändigen Pflichten wie der Meldepflicht nach § 6 TKG ausgenommen werden, wobei der Gesetzgeber hier anscheinend vor allem unternehmensinterne Dienste im Blick hatte.[159] Dieser Gedanke der Verhältnismäßigkeit spricht dafür, auch „offene" Fediverse-Instanzen von den Pflichten des TKG auszunehmen.

5.2.3 Geschäftsmäßig angeboten

Das Fernmeldegeheimnis soll nach dem TDDDG aber auch für die Anbieterinnen von (ganz oder teilweise) geschäftsmäßig angebotenen Telekommunikationsdiensten gelten.[160]

Das „geschäftsmäßige" Erbringen von Telekommunikationsdiensten taucht im TKG inzwischen nicht mehr auf, wurde jedoch in § 3 Nr. 10 TKG a.F. noch definiert als das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht. Eine Fediverse-Instanz könnte durchaus unter diese Definition fallen, sofern die Registrierung auf der Instanz auch Dritten offen steht. Sofern die Instanz dauerhaft betrieben wird, also nicht lediglich für Testzwecke, ist auch von einem nachhaltigen Angebot auszugehen. Indem der deutsche Gesetzgeber auch geschäftsmäßig angebotenen Telekommunikationsdiensten das Fernmeldegeheimnis auferlegt hat, ist er jedoch noch weiter gegangen als die E-Privacy-RL. Nach dem Erwägungsgrund 10 der E-Privacy-RL sollte für nicht öffentlich zugängliche Kommunikationsdienste die Datenschutz-Richtlinie gelten, inzwischen also die DSGVO.[161] Insofern stellt sich die Frage, ob der deutsche Gesetzgeber das Fernmeldegeheimnis auf nicht öffentlich zugängliche, aber geschäftsmäßig erbrachte Kommunikationsdienste erstrecken durfte. Möglicherweise kann diese Frage offen bleiben, weil das Fernmeldegeheimnis im Ergebnis auch aus einer konsequenten Anwendung der DSGVO folgen dürfte. Schließlich ist auch nach der DSGVO keine Rechtsgrundlage nach Art. 6 DSGVO ersichtlich, die das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten

158 Vgl. *Lünenbürger/Stamm*, in: Scheurle/Mayen (Hrsg.), Telekommunikationsgesetz, 3. Aufl. 2018, TKG § 3 Rn. 40; *Ricke*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 4. Aufl. 2019, TKG § 3 Rn. 37.
159 Vgl. BT-Drs. 15/2316, S. 60; Siehe auch *Lünenbürger/Stamm*, in: Scheurle/Mayen (Hrsg.), Telekommunikationsgesetz, 3. Aufl. 2018, TKG § 3 Rn. 41.
160 § 3 Abs. 2 Nr. 2 TDDDG.
161 Art. 94 Abs. 2 DSGVO.

und Verkehrsdaten erlauben würde. Im Ergebnis ist Instanzbetreiberinnen also jedenfalls zu raten, jedenfalls die „direkten Beiträge“ nicht zu überwachen.

5.3 Verantwortlichkeit im Sinne der DSGVO

Verantwortliche ist „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet […]“.[162] Ausschlaggebend nach der DSGVO ist also, wer im konkreten Fall „Herrin der Daten“[163] ist, das heißt, wer die Entscheidungs- oder Verfügungsgewalt über die Daten innehat.[164] Um die Verantwortliche zu identifizieren, kann auch der Wortlaut der Datenschutzrichtlinie bzw. des BDSG von 2003 herangezogen werden, wo die „verantwortliche Stelle“ als jede Person oder Stelle definiert ist, „die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt“.[165]

Die Zwecke der Verarbeitung können als das „Warum“ und „Wofür“ einer Datenverarbeitung beschrieben werden.[166] Diese Zwecke stehen in einem engen Zusammenhang mit der Rechtsgrundlage[167] und sind möglichst konkret zu betrachten.[168] Unter Mittel der Verarbeitung sind beispielsweise bestimmte Verfahren, eine bestimmte Software, eine technische Infrastruktur oder auch eine bestimmte Dienstleisterin zu verstehen.[169] Über die Mittel zu bestimmen, kann auch bedeuten, sonstige Details festzulegen, wie zum Beispiel Löschfristen, die Arten der personenbezogenen Daten[170], Zugangsrechte und Kategorien betroffener Personen.[171]

Die Verantwortlichkeit wird in der Rechtsprechung des EuGH im Interesse eines wirksamen Datenschutzes weit ausgelegt.[172] Wer verantwortlich ist, ist aus der Perspektive einer

---

162 Art. 4 Nr. 7 DSGVO.
163 *Schaffland/Holthaus* in: Schaffland/Wiltfang, DSGVO/BDS, Art. 4 Rn. 145.
164 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 41; *Schreiber*, in: Plath, DSGVO/BDSG/TTDSG, VIII. Verantwortlicher (Nr. 7), Rn. 29.
165 § 3 Abs. 7 BDSG a.F.
166 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 123.
167 Siehe *Radtke* ebd.
168 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 124.
169 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 143.
170 Vgl. EuGH, Urteil vom 10.7.2018 – C-25/17, NJW 2019, 285 (Rn. 70) – Zeugen Jehovas.
171 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 125 f.
172 Siehe nur EuGH, Urteil vom 5.6.2018 – C-210/16, EuZW 2018, 534 (536), Rn. 28 – Wirtschaftsakademie.

durchschnittlichen betroffenen Person zu beurteilen.[173] Es kommt darauf an, was eine betroffene Person vernünftigerweise erwarten kann.[174]

Die Verantwortlichkeit ist im Hinblick auf die konkrete Datenverarbeitung oder Vorgangsreihe zu bestimmen.[175] Nur wenn die verschiedenen Datenverarbeitungen aus technischer Sicht nicht sinnvoll getrennt betrachtet werden können, sind diese zusammen zu beurteilen. Im Zweifel sollten Verarbeitungsvorgänge eher eng gefasst werden, um Verantwortlichkeiten klar abgrenzen zu können.

Verantwortlich ist dabei immer die jeweilige „juristische Einheit", also beispielsweise eine juristische Person.[176]. Wenn also beispielsweise eine Mastodon-Instanz von einem Verein betrieben wird, ist nicht etwa das für die Administration zuständige Vereinsmitglied, sondern der Verein als juristische Person „verantwortlich".

Es können aber auch mehrere Personen gemeinsam verantwortlich sein. Diese müssen dann nach Art. 26 DSGVO eine transparente Vereinbarung darüber treffen, wer welche Pflichten aus der DSGVO erfüllt. Ein maßgebliches Indiz für eine gemeinsame Verantwortlichkeit ist, ob die Personen aus Eigeninteresse Einfluss auf die Verarbeitungen nehmen.[177] Die gemeinsame Verantwortlichkeit ist einerseits abzugrenzen von der getrennten Verantwortlichkeit mehrerer Personen, d. h. die Verantwortlichkeit für unterschiedliche Bereiche, andererseits von der Auftragsverarbeitung.[178]

Es liegt nahe, die Verantwortlichkeit jedenfalls bei den Betreiberinnen einer Instanz zu verorten. Daran schließt sich die Frage an, ob eine gemeinsame Verantwortlichkeit mit weiteren Personen besteht. Daneben besteht allerdings auch die Möglichkeit, dass Instanzbetreiberinnen als Auftragsverarbeiterinnen anzusehen sind. In diesem Fall wären Instanzbetreiberinnen nicht selbst verantwortlich, sodass diese Möglichkeit zuerst zu klären ist.

---

173 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 112.
174 Siehe Erwägungsgrund 47 der DSGVO.
175 Vgl. EuGH, Urteil vom 29.7.2019 – C-40/17, NJW 2019, 2755 (Rn. 74, 76) – Fashion ID; *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 117, 135, 152, 402 f.
176 Siehe *Schaffland/Holthaus*, in: Schaffland/Wiltfang, DSGVO/BDS, Art. 4 Rn. 145; *Schreiber*, in: Plath, DSGVO/BDSG/TTDSG, VIII. Verantwortlicher (Nr. 7), Rn. 28.
177 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 145.
178 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 121.

5.3.1 Abgrenzung zur Auftragsverarbeitung

Zweifel an der Verantwortlichkeit von Instanzbetreiberinnen könnten insofern aufkommen, als dass diese in aller Regel keine eigenen wirtschaftlichen Interessen verfolgen. Betreiberinnen von Mastodon-Instanzen schalten keine personalisierte Werbung und nehmen eine eher neutrale Rolle ein. Dies wird zum Teil als Indiz für eine Auftragsverarbeitung gesehen.[179] Im Falle einer Auftragsverarbeitung wird die Datenverarbeitung den Account-Inhaberinnen als Auftraggeberinnen zugerechnet.

Eine Auftragsverarbeitung zwischen Instanzbetreiberinnen und Account-Inhaberinnen setzt eigentlich voraus, dass die Account-Inhaberinnen selbst Verantwortliche sind. Nach dem Willen des europäischen Parlaments soll die Nutzung sozialer Netzwerke im Rahmen persönlicher oder familiärer Tätigkeiten aber keine Verantwortlichkeit begründen.[180] Im Umkehrschluss liegt eine Verantwortlichkeit der Account-Inhaberinnen nahe, wenn ein soziales Netzwerk nicht rein privat genutzt wird. Schließlich wird ein Social-Media-Account heutzutage häufig als Ersatz für eine eigene Homepage gesehen, welche wiederum eine eigene Verantwortlichkeit begründen würde.[181] Mit ihren Inhalten sprechen Account-Inhaberinnen eine bestimmte Zielgruppe an und entscheiden so über die Kategorien betroffener Personen. Sie führen eine Liste ihrer Followerinnen, die in der Standardeinstellung auch öffentlich zugänglich ist. Zudem veranlassen Account-Inhaberinnen mit ihren Beiträgen andere zu einer Reaktion. Andererseits hat der EuGH auch betont, dass die bloße Nutzung eines sozialen Netzwerks allein nicht unbedingt eine Verantwortlichkeit für die damit verbundenen Datenverarbeitungen begründet.[182] Jedoch können Account-Inhaberinnen zu Verantwortlichen werden, wenn sie über ihren Account personenbezogene Daten von Dritten veröffentlichen.[183]

Der LfDI BaWü betreibt eine Mastodon-Instanz für öffentliche Stellen und Stellen mit Bezug zu öffentlichen Aufgaben und sieht sich in dieser Rolle als Auftragsverarbeiter.[184] Besonders an dieser Instanz ist, dass der LfDI BaWü die Daten auf Weisung der Account-Inhaberinnen

179 Siehe *Hornung*, Datenschutzrechtliche Aspekte der Social Media. In: Hornung/Müller-Terpitz (Hrsg.), Rechtshandbuch Social Media, 2. Aufl., Berlin 2021, S. 152.
180 Siehe Erwägungsgrund 18 DSGVO.
181 Vgl. *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 52.
182 Siehe EuGH, Urteil vom 5.6.2018 – C-210/16, EuZW 2018, 534 (536), Rn. 35 – Wirtschaftsakademie. (zur geographischen Abdeckung s. auch Kurzpapier Nr. 18, S. 5)
183 EuGH, Urteil vom 6. November 2003 – C-101/01 –, juris, Rn. 47.

verarbeitet. Im Fediverse ist es jedoch eher die Ausnahme, dass eine Instanzbetreiberin gegenüber Account-Inhaberinnen weisungsgebunden ist. In aller Regel liegt also keine Auftragsverarbeitung vor.[185] Es besteht aber die Möglichkeit, das Nutzungsverhältnis als Auftragsverarbeitung auszugestalten.

5.3.2 Verantwortlichkeit von Instanzbetreiberinnen

Die Verantwortlichkeit ist in den meisten Fällen bei den Betreiberinnen der jeweiligen Instanz zu verorten. In der Regel wird eine Mastodon-Instanz nicht auf Veranlassung der Account-Inhaberinnen betrieben, sondern für eigene Zwecke. Diese eigenen Zwecke können auch darin bestehen, dass Betreiberinnen einen eigenen Account auf der Instanz besitzen möchten. Instanzbetreiberinnen entscheiden insbesondere über den Einsatz der Software Mastodon. Sie wählen eine bestimmte Infrastruktur aus und installieren und konfigurieren die Software. Damit entscheiden sie über den konkretisierten Zweck sowie über Mittel und Umstände der Datenverarbeitungen.[186] Mit dem Betrieb dieser Software entscheiden die Instanzbetreiberinnen darüber, dass überhaupt personenbezogene Daten in der Datenbank des Servers landen. Das damit geschaffene Risiko ist grundsätzlich den Instanzbetreiberinnen zuzurechnen. Sie sind schließlich auch in der Lage, die Informationen in der Datenbank einzusehen, zu verändern oder zu löschen. Sofern Instanzbetreiberinnen darüber bestimmen, wer sich auf der Instanz registrieren soll oder darf, entscheiden diese auch über die Kategorien personenbezogener Daten. Falls die thematische Ausrichtung einer Instanz festgelegt wird, ist darin ebenfalls eine Entscheidung über Zwecke der Verarbeitung zu sehen.

5.3.3 Auftragsverarbeitung durch Application-Service-Provider

Es ist nicht unüblich, dass eine Instanzbetreiberin einen sog. Application Service Provider mit Installation und Wartung der Instanz beauftragt.[187] In diesem Fall hat die Betreiberin selbst keinen Zugriff auf die Datenbank, sondern lediglich die Dienstleisterin, die den technischen Betrieb der Instanz übernimmt. Dies ändert jedoch nichts daran, dass die Betreiberin über einen

---

184 Siehe https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2022/12/Nutzungsbedingungen-Mastodon_LfDI_V1_1.pdf.
185 Vgl. *Bäcker*, in: Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, 43. Edition, 01.11.2021, DS-GVO Art. 2 Rn. 23.
186 Vgl. *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 143.
187 Beispiele sind https://masto.host/ und https://weingaertner-it.de/index.php/produkt-kategorie/mastodon-hosting/.

Administrationszugang verfügt, also beispielsweise Einblicke in Registrierungsvorgänge und Bestandsdaten von Account-Inhaberinnen erhält. Sie verfügt auch über die Möglichkeit, Beiträge der Account-Inhaberinnen zu löschen. Entscheidend ist jedoch, dass in diesem Fall eine vertragliche Bindung des Application Service Providers besteht. Die Instanzbetreiberin kann diesen dazu anweisen, bestimmte Daten zu löschen oder Auskunft über die Datenverarbeitungen zu geben. Zudem kann die Instanzbetreiberin Einfluss auf die Konfiguration des Servers nehmen. Nur sie ist dazu berechtigt, den Server wieder „abzuschalten". Die Entscheidungsgewalt verbleibt damit bei der Instanzbetreiberin. Es handelt sich hierbei um einen Fall der Auftragsverarbeitung, die den Voraussetzungen des Art. 28 DSGVO zu genügen hat.[188] Insbesondere müssen Instanzbetreiberin und Application-Server-Provider einen Auftragsverarbeitungsvertrag schließen.

5.3.4 Auftragsverarbeitung durch Hosting-Provider

In vielen Fällen wird eine Mastodon-Instanz nicht auf einem eigenen Server betrieben, sondern es wird ein (virtueller) Server bei einem Hosting-Provider gemietet. In der Regel handelt es sich hierbei ebenfalls um eine Auftragsverarbeitung, sodass Instanzbetreiberinnen einen Auftragsverarbeitungsvertrag mit dem Hosting-Provider abschließen müssen.[189] Sofern die Hosting-Provider selbst keinen Zugriff auf den Server haben, sondern nur die technische Infrastruktur bereitstellen, verarbeiten diese selbst auch keine Daten. In diesen wahrscheinlich selteneren Fällen besteht keine Auftragsverarbeitung.

5.3.5 Gemeinsame Verantwortlichkeit von Instanzbetreiberinnen und Entwicklerinnen

Eine Besonderheit des Fediverse liegt darin, dass Entwicklerin und Betreiberin des sozialen Netzwerks in den meisten Fällen nicht die gleiche Person sind. Bei proprietären und zentralisierten Plattformen hingegen fällt die Entwicklung und der Betrieb der Plattform in der Regel in einer Person zusammen. Diese Plattformen werden jeweils von einem bestimmten Unternehmen bzw. einer juristischen Person entwickelt und betrieben. Bei Twitter ist das die X Corp. (vorher: Twitter, Inc.), bei Facebook/Instagram ist es Meta, bei TikTok ByteDance. Im Fediverse ist das in vielerlei Hinsicht anders. Zum einen wird dieses soziale Netzwerk nicht nur

188 Vgl. Gabel/Lutz, in: Taeger/Gabel (Hrsg.), DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 28 DSGVO Rn. 17.
189 Vgl. Gabel/Lutz, in: Taeger/Gabel (Hrsg.), DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 28 DSGVO Rn. 17.

von einem Unternehmen betrieben, sondern von zahlreichen Personen und Organisationen. Zum anderen gibt es eine Vielzahl von Software-Entwicklerinnen von unterschiedlichen Plattformen, wobei hinter einer bestimmten Software sowohl ein einzelnes Unternehmen oder eine ganze Community stehen kann. Die Software „Mastodon“ wird maßgeblich von der Mastodon gGmbH entwickelt, welche zugleich die Instanzen „Mastodon.social“ und „Mastodon.online“ betreibt. In aller Regel handelt es sich bei Entwicklerin und Betreiberin einer Fediverse-Plattform nicht um die selbe Person.

Der Mastodon gGmbH kommt als Entwicklerin ebenfalls eine gewisse Entscheidungsgewalt zu. Sie bestimmt zum Beispiel darüber, welche Informationen im Rahmen der Registrierung erhoben werden oder auf welche Weise die Inhalte übermittelt werden. Die Instanzbetreiberinnen hingegen installieren im Regelfall lediglich die Software auf ihrem Server, ohne große Veränderungen am Code vorzunehmen. Dies legt den Schluss nahe, dass es sich um einen Fall der gemeinsamen Verantwortlichkeit handelt. Ein faktischer Datenzugriff der Mastodon gGmbH ist dafür gerade nicht erforderlich.[190] Die gemeinsame Festlegung der Zwecke und Mittel kann auch darin bestehen, dass sich eine Verantwortliche dem Vorschlag einer anderen anschließt, beispielsweise in Form einer von dieser entwickelten und vorkonfigurierten Software.[191] Indem eine Instanzbetreiberin die Software lokal installiert, macht diese sich den Vorschlag zu eigen.[192]

Dagegen spricht jedoch, dass die Mastodon gGmbH nicht die Zwecke und Mittel der konkreten Datenverarbeitung festlegt. Sie entscheidet insbesondere nicht über Kategorien personenbezogener Daten, zum Beispiel darüber, welche Personen sich auf einer bestimmten Instanz registrieren können. Ab dem Zeitpunkt, in dem die Software lokal installiert wird, fehlt es auch an wesentlichen Einflussmöglichkeiten der Entwicklerin.[193] Die Mastodon gGmbH wäre auch rechtlich gar nicht in Lage, mit Instanzbetreiberinnen vertragliche Vereinbarungen über den Umgang mit Daten zu treffen. Die Software ist schließlich unter der AGPL lizenziert, kann also von allen ohne Einschränkung auf dem eigenen Server installiert und betrieben werden. Damit fehlt es an einer tatsächlichen Entscheidungsbefugnis hinsichtlich der konkretisierten Zwecke und Mittel.[194]

---

190 Vgl. EuGH, Urteil vom 5.6.2018 – C-210/16, EuZW 2018, 534 (Rn. 38) – Wirtschaftsakademie; EuGH, Urteil vom 10.7.2018 – C-25/17, NJW 2019, 285 (Rn. 69) – Zeugen Jehovas; EuGH, Urteil vom 29.7.2019 – C-40/17, NJW 2019, 2755 (Rn. 82) – Fashion ID.
191 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 143.
192 Vgl. *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 143.
193 Vgl. *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 141 f.
194 Vgl. *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 143.

5.3.6 Gemeinsame Verantwortlichkeit von föderierenden Instanzbetreiberinnen

Die Frage, ob föderierende Instanzbetreiberinnen gemeinsam verantwortlich sind, wurde bereits aufgeworfen.[195] Das hätte zur Folge, dass sämtliche Instanzbetreiberinnen eine Vereinbarung miteinander treffen müssten, in der sie festlegen, wer welchen Pflichten aus der DSGVO nachkommt.[196] Damit dürften Instanzen praktisch nur noch im *Limited Federation Mode* betrieben werden. Instanzbetreiberinnen dürften dann nur mit manuell bestätigten Instanzen föderieren, mit denen sie eine solche Vereinbarung abgeschlossen haben. Account-Inhaberinnen könnten ihre Rechte aus der DSGVO gegenüber allen föderierenden Instanzbetreiberinnen geltend machen.[197] Die Instanzbetreiberinnen könnten außerdem für Datenschutzverstöße anderer Instanzbetreiberinnen haften.[198] Bei der Frage, ob eine gemeinsame Verantwortlichkeit vorliegt, müssen jedoch sämtliche Umstände des Einzelfalls berücksichtigt werden.[199] Dazu ist es wichtig, genau zwischen den Datenverarbeitungen bzw. Vorgangsreihen zu differenzieren.

Die gemeinsame Verantwortlichkeit ist jedenfalls abzulehnen für die unter 2.4.1 beschriebenen Datenverarbeitungen. Die auf einer Instanz eingehenden Inhalte werden nicht direkt von der Originalinstanz eingebunden, sondern es wird eine lokale Kopie angelegt. Damit werden beim Lesen von Beiträgen über die eigene Instanz keine Nutzungsdaten an andere Instanzen übermittelt. Es werden auch keine Bestandsdaten übermittelt oder Cookies über Instanzen hinweg ausgelesen (siehe 2.4.2 und 2.4.4). In gewisser Weise „ermöglicht“ eine Mastodon-Instanz den Besuch der Webseite anderer Instanzen. Die Instanzbetreiberinnen bieten einen Zugang zum Fediverse an und damit auch einen Zugang zu den ursprünglich auf anderen Instanzen veröffentlichten Inhalten. Das Folgen eines Accounts oder einer Instanz unterscheidet sich aber nicht wesentlich von dem Abonnement eines RSS-Feed. Das „Ermöglichen“ der Datenverarbeitungen auf anderen Instanzen beschränkt sich darauf, dass der Originalbeitrag oder das originale Accountprofil verlinkt wird. Nach dem Klick auf den Link beginnt ein neuer, klar abgegrenzter Verantwortungsbereich.

---

195 Siehe https://feddit.de/post/466443.
196 Art. 26 Abs. 1 S. 2 DSGVO.
197 Art. 26 Abs. 3 DSGVO.
198 Art. 82 DSGVO.
199 Näher dazu *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 120.

Eine gemeinsame Verantwortlichkeit wäre allerdings denkbar für die Übermittlung der Profilinformationen (2.4.3) und Beiträge (2.4.5.). Die Instanzbetreiberinnen können andere Instanzen blocken und entscheiden so letztlich darüber, an welche anderen Instanzen Inhalte übermittelt werden können. Sie entscheiden außerdem darüber, von welchen anderen Instanzen sie Inhalte empfangen können. Für das Übermitteln und das Abfragen von Inhalten sind also sowohl die versendende Instanz als auch die empfangende Instanz jeweils verantwortlich. Die Frage ist aber, ob darüber hinaus eine gemeinsame Verantwortlichkeit besteht. Nicht jede bloße Übermittlung begründet auch eine gemeinsame Verantwortlichkeit. In der Standardeinstellung werden die Übermittlungen allein durch die Aktivitäten der Account-Inhaberinnen veranlasst. Sofern kein Relay eingebunden wird, fehlt es also an einem kooperativen Element. Die gemeinsame Verantwortlichkeit erfordert jedoch eine gewisse Koordination und nicht bloß eine jeweils kausal gewordene Entscheidung.[200] Darin liegt ihr Unterschied zur zivilrechtlichen Störerhaftung.[201] Bei der „Gemeinsamkeit" handelt es sich um ein offenes Tatbestandsmerkmal, das Raum für Abwägungsentscheidungen im Einzelfall lässt.[202] Die gemeinsame Verantwortlichkeit dient insbesondere dem Zweck, dass sich Personen nicht aus ihrer eigenen Verantwortlichkeit winden können[203] und die Verantwortlichkeit nach der tatsächlichen (aufgeteilten) Entscheidungsbefugnis zugewiesen wird.[204] Auch das Wissen über von anderen durchgeführte Verarbeitungen kann ein Indiz für eine gemeinsame Verantwortlichkeit darstellen.[205] Die Instanzbetreiberinnen haben schließlich einen Überblick über alle „bekannten" Instanzen. Es ist aber grundsätzlich auch für Inhaberinnen eines Mastodon-Accounts transparent, an welche anderen Instanzen ihre Beiträge übermittelt werden.[206] Grundsätzlich werden Beiträge an alle Instanzen übermittelt, auf denen ihnen ein Account folgt. Darüber hinaus besteht in der Regel keine Zusammenarbeit zwischen Instanzbetreiberinnen, um diese Daten beispielsweise für weitere Zwecke zu verwenden. Damit bestehen für Betroffene keine so großen Risiken, welche eine gemeinsame Verantwortlichkeit erforderlich machen würden. Das kann sich allerdings ändern, wenn Beiträge über Threads an Meta übermittelt werden, in dem Wissen, dass die Daten für Werbezwecke verwendet werden. In einem solchen Fall wäre die Frage der gemeinsamen Verantwortlichkeit erneut zu beurteilen.

---

200 Vgl. *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 158.
201 Näher dazu *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 94 f., 102.
202 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 94.
203 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 61 f.
204 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 66.
205 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 113 f.
206 Vgl. Art. 5 Abs. 1 a) DSGVO.

Auch für die Speicherung von Beiträgen auf föderierenden Instanzen sind Instanzbetreiberinnen nicht gemeinsam verantwortlich. Instanzbetreiberinnen sind daher auch nicht verpflichtet, die Löschung von Beiträgen auf anderen Instanzen durchzusetzen, wenn beispielsweise eine automatisierte Löschanfrage fehlgeschlagen ist. Instanzbetreiberinnen haben keinen Einfluss darauf, ob die auf anderen Instanzen kopierten Inhalte tatsächlich gelöscht werden. Für eine gemeinsame Verantwortlichkeit spricht in diesen Fällen die Schutzbedürftigkeit betroffener Personen. Für diese müssen Verantwortliche adressierbar sein.[207] Für betroffene Personen kann es schwer sein, ihre Rechte auf Löschung durchzusetzen, wenn viele Instanzbetreiberinnen nicht einmal ein Impressum besitzen. Eine gemeinsame Verantwortlichkeit zwischen Instanzbetreiberinnen würde auch Anreize für die Entwicklerinnen schaffen, die technischen Probleme bei der Weiterleitung von Löschanfragen zu beseitigen. Ein weiteres Problem tritt auf, wenn Instanzen abgeschaltet werden. Dann bleiben die Beiträge auf anderen Instanzen weiter zugänglich, während sie auf der Originalinstanz von keiner Person mehr gelöscht werden können. Eine gemeinsame Verantwortlichkeit setzt jedoch tatsächliche Einflussmöglichkeiten voraus.[208] Instanzbetreiberinnen verfügen über keinerlei Möglichkeiten, die Beiträge auf anderen Instanzen zu löschen. Account-Inhaberinnen können ihre Rechte auch nicht effektiver geltend machen, wenn sie sich an andere Instanzbetreiberinnen wenden können. Diese können diese Ansprüche überhaupt nicht erfüllen und auch nicht entsprechend auf andere Instanzbetreiberinnen einwirken.[209] Entscheidend ist auch, ob die Instanzbetreiberinnen nach außen (scheinbar) gemeinsam auftreten.[210] Das ist im Fediverse gerade nicht der Fall, da Instanzen verschiedene Software verwenden und auch unterschiedliche Nutzungsbedingungen formulieren. Sie unterscheiden sich also ganz erheblich in ihrem Auftreten. Für Account-Inhaberinnen und auch Aufsichtsbehörden ist klar, an welche Instanzbetreiberinnen sie sich jeweils wenden müssen.[211] Diese Erkennbarkeit der jeweils Verantwortlichen ist ein gewichtiges Argument gegen die Annahme einer gemeinsamen Verantwortlichkeit.[212] Außerdem müssen bei der Auslegung der DSGVO auch die Grundrechte der Instanzbetreiberinnen berücksichtigt werden, insbesondere deren Recht auf Datenschutz. Vor allem Instanzbetreiberinnen, die eine Instanz für sich alleine betreiben, haben eher den Charakter einer Nutzerin. Auch Instanzbetreiberinnen haben ein Recht, eine datenschutzfreundliche Alternative gegenüber

207 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 66.
208 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 101.
209 Vgl. *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 384.
210 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 159.
211 Vgl. Erwägungsgrund 79 der DSGVO.
212 Vgl. *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 68, 79.

kommerziellen sozialen Netzwerken zu nutzen. Sie können aber nur dann vollständige Kontrolle über ihre Daten behalten, wenn diese auch rechtlich dazu in der Lage sind, eine eigene Instanz zu betreiben. Eine gemeinsame Verantwortlichkeit mit anderen Instanzbetreiberinnen würde Instanzbetreiberinnen auch davon abschrecken, anderen Personen einen Account auf ihrer Instanz zur Verfügung zu stellen. Das würde Account-Inhaberinnen auf werbefinanzierte soziale Netzwerke zurückwerfen.

5.3.7 Gemeinsame Verantwortlichkeit von Instanzbetreiberinnen und Account-Inhaberinnen

Auch die gemeinsame Verantwortlichkeit von Instanzbetreiberinnen und Account-Inhaberinnen muss im Hinblick auf die konkrete Datenverarbeitung beurteilt werden. Sie liegt jedenfalls in den Fällen nahe, in denen Account-Inhaberinnen auch unabhängig von Instanzbetreiberinnen verantwortlich sind. In Ausnahmefällen ist eine eigenständige Verantwortlichkeit von Account-Inhaberinnen aber gar nicht erforderlich, um eine gemeinsame Verantwortlichkeit zu begründen.[213]

Die EuGH-Rechtsprechung scheint eine gemeinsame Verantwortlichkeit hinsichtlich der Datenverarbeitungen beim Besuch der Webseite (2.4.1.) nahezulegen. Eine gemeinsame Verantwortlichkeit setzt nicht voraus, dass jede Verantwortliche Zugang zu diesen personenbezogenen Daten hat.[214] Es muss auch nicht jeder in gleicher Weise die Kontrolle über die Verarbeitung haben.[215] Im Fall von Facebook war es ausreichend, dass den Facebook-Seitenbetreiberinnen anonyme Statistiken zur Verfügung gestellt wurden.[216] Das Urteil betraf allerdings das Webtracking mittels Cookies, mit dem die Beteiligten gemeinsame wirtschaftliche Interessen verfolgten.[217] Facebook dient die Funktion dazu, ihr System der Werbung zu verbessern.[218] Den Account-Inhaberinnen ermöglicht es anhand der Statistiken Kenntnis von den Persönlichkeitsprofilen ihrer Besucherinnen zu erhalten.[219]Damit können Facebook-

213 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 160.
214 Siehe EuGH, Urteil vom 5.6.2018 – C-210/16, EuZW 2018, 534 (Rn. 38) – Wirtschaftsakademie; EuGH, Urteil vom 10.7.2018 – C-25/17, NJW 2019, 285 (Rn. 69) – Zeugen Jehovas; EuGH, Urteil vom 29.7.2019 – C-40/17, NJW 2019, 2755 (Rn. 82) – Fashion ID.
215 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 47.
216 Siehe EuGH, Urteil vom 5.6.2018 – C-210/16, EuZW 2018, 534 (536), Rn. 34; *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 163.
217 Siehe EuGH, Urteil vom 5.6.2018 – C-210/16, EuZW 2018, 534 (Rn. 36) – Wirtschaftsakademie.
218 Siehe EuGH, Urteil vom 5.6.2018 – C-210/16, EuZW 2018, 534 (Rn. 59) – Wirtschaftsakademie.
219 Siehe EuGH, Urteil vom 5.6.2018 – C-210/16, EuZW 2018, 534 (Rn. 33 f.) – Wirtschaftsakademie.

Seitenbetreiberinnen ihre Inhalte spezifisch auf eine bestimmte Zielgruppe ausrichten.[220] Auf diese Weise tragen Facebook-Seitenbetreiberinnen zur Verarbeitung der personenbezogenen Daten bestimmter Seitenbesucherinnen bei und fördern diese aktiv[221] Die Seitenbetreiberinnen können auch die Vermarktung steuern, indem sie mithilfe von Filtern Kriterien festlegen, nach denen die Statistiken erstellt werden (z. B. demografische Daten über die Zielgruppe), und Kategorien von Personen bezeichnen, deren personenbezogene Daten von Facebook ausgewertet werden.[222] In diesem Fall zahlen Facebook-Seitenbetreiberinnen sogar Geld für eine konkrete Zusammenarbeit mit Facebook. Hier bestimmen also Facebook und Seitenbetreiberinnen ganz klar gemeinsam über den konkreten Zweck der Datenverarbeitung, indem sie einen Vertrag über personalisierte Werbung abschließen.[223] Für den EuGH war diese sog. Parametrierung entscheidend, um über die bloße Nutzung einer vorkonfigurierten Plattform hinaus eine (Mit-)Verantwortlichkeit von Account-Inhaberinnen zu begründen.[224] Die Inhaberinnen eines Mastodon-Accounts hingegen können nicht beeinflussen, welchen Zielgruppen ihre Beiträge angezeigt werden. Dies hängt in erster Linie davon ab, ob andere Account-Inhaberinnen mit den Inhalten interagieren. Inhaberinnen von Mastodon-Accounts erhalten auch keine Statistiken über ihre Besucher. Ähnlich gelagert ist dies bei dem „Social Plugin", der Einbettung von Facebook-Webseiten in die eigene Homepage.[225] Auch in diesem Fall dienten die Datenverarbeitungen dazu, die Werbung der Webseitenbetreiberin in Facebook zu optimieren.[226] Prinzipiell können auch Mastodon-Beiträge in Webseiten eingebunden werden. Dies dient jedoch nicht dem Zweck, Informationen über Besucherinnen der Webseite zu erhalten.

Zum Teil wird eine gemeinsame Verantwortlichkeit schon darin gesehen, dass Account-Inhaberinnen die Plattform mit eigenen Inhalten befüllen und so für eigene Zwecke nutzen.[227] Nach einem solchen Verständnis könnte sich die gemeinsame Verantwortlichkeit auch auf weitere Datenverarbeitungen erstrecken. Account-Inhaberinnen könnten schließlich ihre Besucherinnen dazu animieren, sich auf der gleichen Instanz zu registrieren. Dadurch tragen sie

---

220 Siehe OVG Schleswig, Urteil vom 25.11.2021 – 4 LB 20/23, ZD 2022, 344 (348), Rn. 144.
221 Siehe EuGH ebd.
222 Siehe EuGH, Urteil vom 5.6.2018 – C-210/16, EuZW 2018, 534 (536), Rn. 36 – Wirtschaftsakademie.
223 Vgl. EuGH, Urteil vom 5.6.2018 – C-210/16, EuZW 2018, 534 (Rn. 32) – Wirtschaftsakademie.
224 Siehe EuGH, Urteil vom 5.6.2018 – C-210/16, EuZW 2018, 534 (536), Rn. 36; *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 127.
225 Siehe EuGH, Urteil vom 29.7.2019 – C-40/17, NJW 2019, 2755 (Rn. 75) – Fashion ID.
226 Vgl. EuGH, Urteil vom 29.7.2019 – C-40/17, NJW 2019, 2755 (Rn. 80) – Fashion ID.
227 Vgl. OVG Schleswig, Urteil vom 25.11.2021 – 4 LB 20/23, ZD 2022, 344 (348), Rn. 144; *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 184.

dazu bei, dass die Instanzbetreiberinnen Bestandsdaten erhalten. Ohne die Beiträge der Account-Inhaberinnen würden andere nicht darauf reagieren und ebenfalls Beiträge zurück an die Instanz senden. Derartige Erwägungen haben in der Rechtsprechung des EuGH aber keine Rolle gespielt.

Sofern überhaupt eine Verantwortlichkeit von Account-Inhaberinnen besteht, kann in der Regel von getrennten Verantwortungsbereichen ausgegangen werden. Je nachdem wie stark Instanzbetreiberinnen und Account-Inhaberinnen zusammenwirken, können sie auch gemeinsam verantwortlich sein. Dann müssen sie auch eine transparente Vereinbarung nach Art. 26 DSGVO treffen. Wichtig ist in jedem Fall, dass bei der konkreten Ausgestaltung keine Schutzlücke für betroffene Personen entsteht.

6. Pflichten gegenüber Besucherinnen der Instanz

Unter dem Punkt 2.4.1 wurde deutlich, dass bereits beim Besuch einer Mastodon-Instanz bestimmte Daten verarbeitet werden, die potenziell der Besucherin zugeordnet werden können. Aus Sicht der Betreiberinnen stellt sich die Frage, welche datenschutzrechtlichen Pflichten sie gegenüber ihren Besucherinnen haben, oder umgekehrt, welche Rechte die Besucherinnen gegenüber Instanzbetreiberinnen geltend machen können.

6.1 Anwendbarkeit von DSGVO und TDDDG

Im Datenschutzrecht gibt es kein „belangloses" Datum.[228] Obwohl die beim Besuch einer Fediverse-Instanz verarbeiteten Daten eher technischer Natur sind, sind grundsätzlich alle personenbezogenen oder personenbeziehbaren Informationen vom Datenschutzrecht erfasst.[229] Das betrifft auch die vom User-Agent mitgelieferten Daten über den verwendeten Browser oder die verwendete App, das Betriebssystem, die Prozessorarchitektur und die im Browser eingestellte Sprache. Für sich genommen lassen diese Informationen, ebenso wie die eingegebene URL und der Zeitpunkt des Zugriffs, keinen Rückschluss auf eine bestimmte Person zu. Wenn diese Daten jedoch mit einer IP-Adresse verknüpft werden, können sie einer identifizierbaren Person zugeordnet werden.

Auch dynamische IP-Adressen sind aus der Perspektive der Instanzbetreiberinnen personenbeziehbare Daten. Eine Instanzbetreiberin verfügt zwar nicht ohne Weiteres über das Zusatzwissen, um von einer IP-Adresse auf eine bestimmte Person zu schließen. Theoretisch könnten Instanzbetreiberinnen jedoch Auskunftsansprüche gegenüber den Internetprovidern geltend machen, zum Beispiel um Verursacherinnen eines DDoS-Angriffs zu identifizieren. Sie können auch gemäß § 24 TDDDG auskunftspflichtig gegenüber Ermittlungsbehörden und Geheimdiensten sein, welche ohne Weiteres einen Personenbezug herstellen können.

In Bezug auf „Cookies" wie die _mastodon_session ist § 25 TDDDG anzuwenden. Die Regelungen der Umsetzung von Art. 5 Abs. 3 der E-Privacy-RL haben grundsätzlich Vorrang vor

228 So schon das BVerfG, Urteil vom 15.12.1983 – 1 BvR 209/83 u. a., NJW 1984, 419 (422).
229 *Gola*, in Gola/Heckmann (Hrsg.), DS-GVO – BDSG, 3. Aufl. 2022, Art. 4 DS-GVO Rn. 6.

der DSGVO.[230] Es bedarf jedenfalls für die Speicherung und das Auslesen der Cookies keiner zusätzlichen Rechtsgrundlage aus der DSGVO. Für eine Weiterverarbeitung der Daten, beispielsweise zur Reichweitenanalyse, wäre hingegen eine zusätzliche Erlaubnisnorm aus der DSGVO erforderlich.[231]

Die sogenannte Haushaltsausnahme, nach der ausschließlich persönliche oder familiäre Tätigkeiten vom Anwendungsbereich der DSGVO ausgenommen werden, kommt Instanzbetreiberinnen nur in wenigen Fällen zugute. Als Ausnahmevorschrift ist diese eng zu verstehen. Sobald eine Instanzbetreiberin Informationen von Account-Inhaberinnen öffentlich macht, besteht für die Haushaltsausnahme kein Raum.[232] Ausnahmsweise kann sie eingreifen, wenn Instanzbetreiberinnen keine Registrierung erlauben und zugleich die Einstellung DISALLOW_UNAUTHENTICATED_API_ACCESS aktiviert haben. In diesem Fall müssen Instanzbetreiberinnen insbesondere § 19 TDDDG beachten. Im Ergebnis ergibt sich also für alle Instanzbetreiberinnen die Vorgabe, die bei dem Besuch der Webseite verarbeiteten Daten nur insoweit zu verarbeiten, wie dies notwendig ist.[233]

6.2 Rechtsgrundlagen für die Datenverarbeitung

Auch die beim Besuch einer Fediverse-Instanz notwendigen Datenverarbeitungen müssen von einer Erlaubnisnorm gedeckt sein.[234]

6.2.1 Verarbeitung von Nutzungsdaten

Die Verarbeitung der IP-Adresse, der eingegebenen URL, des Zugriffszeitpunkts und der im User-Agent mitgelieferten Daten sollte nicht auf eine Einwilligung nach Art. 6 Abs. 1 a) DSGVO gestützt werden. Grundsätzlich kann eine Einwilligung durch eine „eindeutige bestätigende Handlung“ erteilt werden.[235] Es ließe sich insofern argumentieren, dass sich Besucherinnen einer Instanz mit dem Aufruf der Webseite einverstanden erklären, dass die dafür notwendigen Daten übermittelt werden. Einer durchschnittlichen Instanzbesucherin kann das Wissen darüber,

230 *Schmitz*, in: Geppert/Schütz (Hrsg.), Beck’scher TKG-Kommentar, 5. Aufl. 2023, TTDSG § 25 Rn. 1, 11.
231 Vgl. *Piltz*, in: Plath (Hrsg.), DSGVO/BDSG/TTDSG, 4. Auflage 2023, c) Verhältnis in Bezug auf Verarbeitungsphasen, Rn. 14.
232 Vgl. EuGH, Urteil vom 6. November 2003 – C-101/01 –, juris (Rn. 47).
233 Vgl. *Schneider*, in: Assion (Hrsg.), TTDSG, § 19 Rn. 14.
234 Art. 5 Abs. 1 a) DSGVO.
235 Siehe *Frenzel*, in: Paal/Pauly (Hrsg.), DS-GVO, 3. Aufl. 2021 DS-GVO Art. 6 Rn. 11.

welche Datenverarbeitungen wirklich notwendig sind, aber nicht unbedingt unterstellt werden. Im Übrigen kann die Besucherin nicht in Datenverarbeitungen einwilligen, von denen sie nichts weiß.

Diese Datenverarbeitungen sind vielmehr vom berechtigten Interesse der Instanzbetreiberinnen nach Art. 6 Abs. 1 f) DSGVO gedeckt. Im Rahmen dieser Erlaubnisnorm ist immer eine Interessenabwägung erforderlich. Instanzbetreiberinnen haben das berechtigte Interesse, dass die Webseite ihrer Fediverse-Instanz abgerufen werden kann, zum Beispiel damit ihr Profil oder die URL zu einem Beitrag aufgerufen werden kann. Das berechtigte Interesse kann aber auch darin bestehen, anderen Personen die Möglichkeit zu eröffnen, einen Account auf der Instanz zu nutzen. Demgegenüber steht ein eher geringes Interesse der betroffenen Person, da diese Daten nur kurzzeitig gespeichert werden.

Eine längere Speicherung dieser Daten über die notwendige Dauer hinaus bedarf hingegen einer gesonderten Rechtfertigung.[236] Teilweise wird die Speicherung von Log-Dateien damit begründet, dass sie dazu verwendet werden können, Distributed-Denial-of-Service (DDoS)-Angriffe zu verhindern.[237] Zum Beispiel können die IP-Adressen der Angreiferinnen auf eine Sperrliste gesetzt werden.[238] Ein weiteres Argument ist die potenzielle Speicherung und Identifizierbarkeit der Angreiferinnen als Abschreckungsmaßnahme.[239] Es ist jedoch sehr zweifelhaft, ob solche Maßnahmen überhaupt geeignet sind. Darüber hinaus können Daten wie die IP-Adresse und die vom User-Agent mitgelieferten Daten auch für die Fehleranalyse verwendet werden. Dieses Interesse der Instanzbetreiberinnen kann allerdings höchstens eine kurze Speicherdauer rechtfertigen. Im Sinne des Grundsatzes der Speicherbegrenzung sollten daher die Log-Dateien auf dem Server regelmäßig gelöscht oder am besten gar nicht gespeichert werden (Art. 5 Abs. 1 e) DSGVO).

6.2.2 Einbetten von Medien anderer Webseiten

Das Einbetten von Medien anderer Webseiten, insbesondere von Youtube-Videos, erfolgt ebenfalls im Rahmen des berechtigten Interesses gem. Art. 6 Abs. 1 f) DSGVO. Dadurch, dass

236 Art. 5 Abs. 1 c) und e) DSGVO.
237 Vgl. BGH, Urteil vom 16. Mai 2017 – VI ZR 135/13 –, BGHZ 215, 55-69.
238 Siehe https://docs.joinmastodon.org/admin/moderation/#blocking-by-ip.
239 Vgl. BGH, Urteil vom 16. Mai 2017 – VI ZR 135/13 –, BGHZ 215, 55-69.

die Verbindung zu Youtube erst nach einem Klick auf das zwischengespeicherte Vorschaubild erfolgt, sind die Interessen und Grundrechte der betroffenen Person nur in geringem Maße beeinträchtigt. Dem steht das Interesse der Instanzbetreiberin entgegen, eine komfortable, den Erwartungen der Account-Inhaberinnen entsprechende, Webseite anzubieten. Die Interessenabwägung fällt somit zugunsten der Instanzbetreiberin aus. Noch eindeutiger wäre dieses Ergebnis, wenn die PreviewCard auch eine Warnung enthalten würde, dass mit dem Abspielen des eingebetteten Videos eine fremde Webseite abgerufen wird. Dies würde für Besucherinnen der Instanz noch deutlicher machen, dass lediglich das Vorschaubild, nicht aber das ganze Video auf der Instanz zwischengespeichert wird.

6.2.3 Verarbeitung von „Cookies"

Ein „Cookie-Banner" ist auf einer Mastodon-Instanz im Normalfall nicht erforderlich. Das Speichern von Informationen im lokalen Speicher bedarf zwar vom Grundsatz her einer Einwilligung durch die Besucherin, ebenso wie der Zugriff auf diese Informationen (§ 25 Abs. 1 TDDDG). Dies gilt unabhängig davon, welchen Zweck das „Cookie" verfolgt oder ob der Local Storage oder der Session Storage genutzt wird. Eine Ausnahme gilt aber, wenn das „Cookie" unbedingt erforderlich ist, um einen von der Nutzerin ausdrücklich gewünschten digitalen Dienst zur Verfügung zu stellen. Das ist spätestens mit den neueren Mastodon-Versionen der Fall, in denen die _mastodon_session erst mit Aufruf der Registrierungs- oder Loginseite gespeichert wird. Personen, die eine Mastodon-Instanz im Browser aufrufen, wollen ausdrücklich diese Website in Anspruch nehmen. Es handelt sich um integrative Bestandteile der Software Mastodon, die einen klar eingeschränkten, technischen Zweck verfolgen. Die Ausnahmevorschrift in § 25 Abs. 2 Nr. 2 TDDDG erlaubt es daher, die Cookies _session_id und _mastodon_session zu verwenden.

6.3 Informations- und Auskunftsrechte

Die in den Datenschutzhinweisen erforderlichen Informationen ergeben sich aus Art. 13 DSGVO. In aller Regel ist es erforderlich, Namen und Kontaktdaten der Verantwortlichen sowie gegebenenfalls der Vertreterin anzugeben. Weiterhin sind die Zwecke und die Rechtsgrundlage der jeweiligen Datenverarbeitung zu beschreiben. Auch das berechtigte Interesse an der Datenverarbeitung ist darzulegen. Zusätzlich ist die Speicherdauer anzugeben, insbesondere in

Bezug auf die Server-Logs. Die betroffenen Personen sind außerdem über ihre Rechte zu unterrichten.

Schwieriger zu beantworten ist die Frage, wie Instanzbetreiberinnen die Auskunftspflichten aus Art. 15 DSGVO erfüllen können. Es ist Instanzbetreiberinnen nicht ohne Weiteres möglich, einer Besucherin ohne Fediverse-Account mitzuteilen, ob zu dieser Person Nutzungsdaten gespeichert sind. Eine Instanzbetreiberin müsste zunächst gegenüber sämtlichen Internetprovidern Auskunftsanfragen stellen, um sämtliche IP-Adressen einer Person zuordnen zu können. Das wäre nicht nur ein kaum zu bewältigender Aufwand für Instanzbetreiberinnen, sondern auch Eingriff in die Rechte aller anderen Instanzbesucherinnen. Eine Auskunft ist lediglich dann möglich, wenn die anfragende Person in der Anfrage selbst eine IP-Adresse nennt und um Auskunft darüber bittet, ob diese IP-Adresse und weitere Daten gespeichert sind. Da dynamische IP-Adressen jedoch ständig neu vergeben werden, ist der Aussagegehalt einer solchen Auskunft gering. Die einfachste Lösung für dieses Problem besteht darin, von vornherein keine IP-Adressen zu erheben oder Server-Logs regelmäßig zu löschen, sodass im Falle einer Anfrage eine negative Auskunft gegeben werden kann.

6.4 Recht auf Löschung und Widerspruchsrecht

Das Recht auf Löschung oder das „Recht auf Vergessenwerden“ bereitet ähnliche Schwierigkeiten wie das Recht auf Auskunft. Instanzbetreiberinnen können IP-Adressen nicht ohne Weiteres der anfragenden Person zuordnen. Auch dieses Problem lässt sich dadurch umgehen, indem Server-Logs regelmäßig gelöscht werden. Sofern dies in der Vergangenheit versäumt wurde, kann eine Löschanfrage zum Anlass genommen werden, die Logdateien zu löschen und idealerweise eine automatisierte Löschung einzurichten. Das gleiche gilt, wenn betroffene Personen von ihrem Widerspruchsrecht aus Art. 21 Abs. 1 DSGVO Gebrauch machen. Es wird Instanzbetreiberinnen nicht gelingen, schutzwürdige Gründe für die weitere Verarbeitung der Nutzungsdaten nachzuweisen. Es empfiehlt sich daher, auch im Falle eines Widerspruchs mit der Löschung aller Log-Dateien zu reagieren.

7. Pflichten gegenüber Account-Inhaberinnen auf der eigenen Instanz

Instanzbetreiberinnen verarbeiten vor allem Daten derjenigen Personen, die auf ihrer Instanz einen Account besitzen. Die bei der Registrierung verarbeiteten Daten (siehe 2.4.2) können als Bestandsdaten bezeichnet werden. Bei den im Rahmen eines Log-ins verarbeiteten Daten (siehe 2.4.4) handelt es sich um Nutzungsdaten, während sich die unter 2.4.3 und 2.4.5 beschriebenen Vorgänge auf Inhaltsdaten beziehen.

7.1 Anwendbarkeit von DSGVO und TDDDG

Für den _session_id-Cookie, der im Rahmen des Login-Prozesses im Browser der Account-Inhaberinnen gespeichert wird, gilt die „Cookie-Regelung“ in § 25 TDDDG.

„Direkte Beiträge“ dürften regelmäßig dem Fernmeldegeheimnis unterliegen (siehe 5.2.3). Da Fediverse-Instanzen jedoch in der Regel keine „öffentlich zugänglichen“ Telekommunikationsdienste sind, ist auch in Bezug auf direkte Beiträge die DSGVO zu beachten.

Auch im Übrigen findet die DSGVO Anwendung. Für die Haushaltsausnahme besteht im Verhältnis zu Account-Inhaberinnen kein Raum. Sobald Instanzbetreiberinnen anderen Personen Accounts zur Verfügung stellen, wird die Instanz nicht mehr rein für persönliche Zwecke genutzt. Eine Ausnahme ist denkbar, wenn die Instanz nur einem sehr kleinen Familien- oder Freundeskreis offen steht. In diesem Fall müssen jedenfalls die technischen und organisatorischen Vorkehrungen nach § 19 TDDDG getroffen werden.

7.2 Rechtsgrundlagen für die Datenverarbeitung

7.2.1 Verarbeitung von „Cookies“

Die Rechtsgrundlage für die Nutzung des lokalen Speichers durch die _session_id ist § 25 Abs. 2 Nr. 2 TDDDG. Dieser „Cookie“ hat den Zweck, dass Account-Inhaberinnen sich beim nächsten Besuch der Website nicht erneut einloggen müssen. Damit, dass Account-

Inhaberinnen sich am Ende eines Besuchs nicht ausloggen, äußern sie den ausdrücklichen Wunsch, sich beim nächsten Besuch nicht wieder einloggen zu müssen.

7.2.2 Verarbeitung von Nutzungsdaten

Fraglich ist, ob die Speicherung der letzten verwendeten IP-Adresse von einem berechtigten Interesse der Instanzbetreiberinnen gedeckt ist. Die IP-Adresse kann insbesondere dazu benötigt werden, um diese für die Registrierung zu sperren.[240] Damit soll verhindert werden, dass sich Spam-Accounts nach einer Sperrung erneut registrieren können. Der Nutzen dieser Maßnahme ist fraglich, da es zahlreiche Wege gibt, eine solche IP-Sperre zu umgehen. Diesem Interesse der Instanzbetreiberinnen an der Speicherung stehen die Interessen der Account-Inhaberinnen entgegen, insbesondere deren Recht auf Datenschutz. Instanzbetreiberinnen können zwar anhand einer IP-Adresse die Account-Inhaberinnen nicht identifizieren, sofern sie gegenüber deren Internetprovider keinen Auskunftsanspruch haben. Es besteht jedoch beispielsweise die Möglichkeit, dass die Datenbank des Servers oder der Administrationszugang von Ermittlungsbehörden (rechtswidrig) beschlagnahmt wird, für die eine Identifizierung ohne Weiteres möglich ist.[241] Im Rahmen einer Interessenabwägung überwiegt das Interesse der Account-Inhaberinnen an einer anonymen Nutzung ihres Fediverse-Accounts. Es fehlt damit an einer Rechtsgrundlage für die Speicherung von IP-Adressen der Account-Inhaberinnen.

7.2.3 Verarbeitung von Bestandsdaten

Die Verarbeitung der Bestandsdaten dürfte erforderlich sein, damit Account-Inhaberinnen die Instanz nutzen können. Instanzbetreiberinnen stehen aber vor der Frage, welche Rechtsgrundlage sie hierfür heranziehen können.

Es ist möglicherweise nicht empfehlenswert, diese Datenverarbeitungen auf eine pauschale Einwilligung nach Art. 6 Abs. 1 a) DSGVO zu stützen. Eine Einwilligung wird insbesondere dadurch suggeriert, dass im Registrierungsformular das Einverständnis zu den Datenschutzhinweisen abgefragt wird. An eine solche Einwilligung werden jedoch strenge Voraussetzungen gestellt. Instanzbetreiberinnen müssten insbesondere die Einwilligungen der

240 https://docs.joinmastodon.org/methods/admin/ip_blocks/.
241 Ein solcher Fall hat sich erst kürzlich bei einer US-amerikanischen Instanz ereignet, siehe https://kolektiva.social/@admin/110637031574056150.

Account-Inhaberinnen dokumentieren und gegebenenfalls den Aufsichtsbehörden nachweisen können.[242] Allein aus der Tatsache, dass eine Registrierung ohne Setzen des Häkchens nicht möglich ist, lässt sich eine pauschale Einwilligung in alle Datenverarbeitungsvorgänge jedenfalls nicht herleiten. Es wird insbesondere nicht ersichtlich, auf welche Version der Datenschutzhinweise sich die Einwilligung bezieht und ob diese zwischenzeitlich geändert wurde. Die Administrationsoberfläche von Mastodon stellt für eine solche Dokumentation keine ausreichenden Mittel bereit. Es stellt Instanzbetreiberinnen daher vor große Herausforderungen, die Anforderungen an eine Einwilligung zu erfüllen.

Die Rechtsgrundlage ist vielmehr in Art. 6 Abs. 1 b) DSGVO zu sehen.[243] Dafür ist es nicht unbedingt erforderlich, dass zwischen den Personen ein Vertrag im Sinne des deutschen BGB geschlossen wurde. In vielen Fällen können Zweifel an dem für einen Vertragsschluss notwendigen rechtlichen Bindungswillen von Instanzbetreiberinnen und Account-Inhaberinnen bestehen. Schließlich werden Instanzen oft ehrenamtlich oder im Rahmen gegenseitiger Hilfe betrieben. Die Instanzbetreiberinnen möchten sich in der Regel nicht rechtlich binden und die ständige Verfügbarkeit der Instanz gewährleisten. Für einen Rechtsbindungswillen spricht jedoch, dass Instanzbetreiberinnen von Account-Inhaberinnen einfordern, die Nutzungsbedingungen und Verhaltensregeln zu beachten.[244] Account-Inhaberinnen wiederum haben ein Interesse daran, dass eine Instanz nicht von heute auf morgen abgeschaltet wird.

Auch wenn diese Frage bislang nicht vom EuGH geklärt wurde, ist davon auszugehen, dass Art. 6 Abs. 1 b) DSGVO auch „vertragsähnliche“ Verhältnisse erfasst. Klar ist, dass diese Erlaubnisnorm eng zu verstehen ist, insbesondere in Hinblick auf die Erforderlichkeit der Datenverarbeitung.[245] Hinter Art. 6 Abs. 1 b) DSGVO steht der Gedanke, dass bereits ein Vertragsschluss auf einer selbstbestimmten Entscheidung der Beteiligten beruht, welche die dafür notwendigen Datenverarbeitungen rechtfertigt.[246] Dieser Gedanke lässt sich auch auf vertragsähnliche Vertrauensverhältnisse übertragen, wie Gefälligkeiten oder Mitgliedschaften in

---

242 Siehe Kurzpapier Nr. 20 der Datenschutzkommission zur Einwilligung nach der DS-GVO, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_20.pdf.

243 So sieht es auch *Riemann* im Mastodon Privacy Policy Generator, https://blog.riemann.cc/projects/mastodon-privacy-policy-generator/.

244 Vgl. *Kreutz*, ZUM 2018, 162 (166 f.).

245 Siehe nur EuGH Urteil vom 4. Juli 2023 – C 252/21, Rn. 93, 98 f.

246 Siehe *Buchner/Petri*, in: Kühling/Buchner (Hrsg.), DS-GVO BDSG, 3. Aufl. 2020, DSGVO Art. 6 Rn. 30; *Albers/Veit*, in: Wolff/Brink/v. Ungern-Sternberg (Hrsg.), BeckOK Datenschutzrecht, 44. Edition, Stand: 01.05.2023, DS-GVO Art. 6 Rn. 41.

Vereinen.[247] Dazu zählt auch die Entscheidung, einen Account auf einer Fediverse-Instanz zu nutzen und die dafür erforderlichen Datenverarbeitungen zuzulassen. Instanzbetreiberinnen müssen bestimmte Daten verarbeiten, um Account-Inhaberinnen die Nutzung ihres Accounts zu ermöglichen.

Ein Problem kann sich dann ergeben, sobald sensible Informationen verarbeitet werden. Für besondere Kategorien personenbezogener Daten gilt nach Art. 9 DSGVO ein generelles Verarbeitungsverbot. Schon die Bestandsdaten eines Accounts können sensible Informationen darstellen, wenn sich eine Person beispielsweise auf einer LGTBQ-Instanz oder auf einer „Mental-Health"-Instanz registriert. In diesen Fällen kann schon allein von der Registrierung auf dieser Instanz auf die sexuelle Orientierung oder Gesundheitsdaten der Account-Inhaberinnen geschlossen werden. Aber auch politische Meinungen zählen zu den besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO. Schwierig wird es auch, wenn sich das sensible Datum bereits aus dem Domainnamen oder der thematischen Ausrichtung der Instanz ergibt. Die Information, auf welcher Instanz sich eine Person registriert hat, ist stets öffentlich. Instanzbetreiberinnen verfügen jedoch zusätzlich über weitere Informationen, insbesondere eine E-Mail-Adresse. In dieser Kombination werden die Informationen gerade nicht „offensichtlich öffentlich" gemacht. Vielen Beitreiberinnen von Mastodon-Instanzen kommt allerdings zugute, dass sie keine Gewinnerzielungsabsichten verfolgen, sondern Instanzen gerade bereitstellen, um Account-Inhaberinnen eine Alternative zu datenschutzgefährdenden sozialen Netzwerken zu bieten. Politische, weltanschauliche, religiöse oder gewerkschaftlich ausgerichtete Organisationen ohne Gewinnerzielungsabsicht können sich zur Verarbeitung von Bestandsdaten auf die Erlaubnis in Art. 9 Abs. 2 d) DSGVO beziehen. Dies gilt unabhängig von ihrer Rechtsform. Für andere Organisationen oder Einzelpersonen ist es hingegen nicht empfehlenswert, solche Instanzen zu betreiben, deren Domain-Name oder thematische Ausrichtung Rückschlüsse auf sensible Informationen zulässt.

247 Vgl. Buchner/Petri, in: Kühling/Buchner (Hrsg.), DS-GVO BDSG, 3. Aufl. 2020, DSGVO Art. 6 Rn. 30; Albers/Veit, in: Wolff/Brink/v. Ungern-Sternberg (Hrsg.), BeckOK Datenschutzrecht, 44. Edition, Stand: 01.05.2023, DS-GVO Art. 6 Rn. 42; Kritisch dazu Schulz, in: Gola/Heckmann (Hrsg.), DS-GVO – BDSG. Kommentar, 3. Aufl. 2022, DS-GVO Art. 6, Rn. 33.

7.2.4 Weitere Profildaten und Interaktion auf der Instanz

Die Erlaubnisnorm des Art. 6 Abs. 1 b) DSGVO ist eng zu verstehen und erfasst nur die zur Erfüllung des „Vertrages“ erforderlichen Daten. Neben den Bestandsdaten müssen die Instanzbetreiberinnen auch die Inhaltsdaten verarbeiten, um Account-Inhaberinnen die Nutzung ihres Accounts zu ermöglichen. Das betrifft insbesondere die Verarbeitung von Profilinformationen sowie die Veröffentlichung der von Account-Inhaberinnen verfassten Beiträge und deren Übermittlung an andere Fediverse-Instanzen. Auch die Übermittlung der Beiträge an andere Fediverse-Instanzen ist Gegenstand des zwischen Instanzbetreiberin und Account-Inhaberin geschlossenen Nutzungsvertrags. Insofern ist diese Übermittlung auch dann zulässig, wenn eine in Drittländern betriebene Instanz mit der eigenen Instanz föderiert.[248] Es kann aber auch schon bezweifelt werden, dass es sich hierbei überhaupt um eine „Übermittlung“ im Sinne der Art. 44 ff. DSGVO handelt. Jede im Internet veröffentlichte Website kann auf der ganzen Welt abgerufen werden, worin jedoch noch keine Übermittlung in Drittländer zu sehen ist.[249] Ähnlich verhält es sich, wenn Informationen von anderen Fediverse-Instanzen abgerufen werden.

Riemann geht in dem Mastodon Privacy Policy Generator davon aus, dass die Verarbeitung von weiteren Profilinformationen, insbesondere Anzeigename und Profilbild, nicht zwingend erforderlich ist, um den Nutzungsvertrag zu erfüllen.[250] Insofern bereitet es auch Schwierigkeiten, eine Erlaubnisnorm für die Verarbeitungen weiterer Inhaltsdaten zu finden, die mit der Interaktion auf der Instanz einhergehen (siehe 2.4.5).

Art. 6 Abs. 1 b) DSGVO bietet jedenfalls dann keine ausreichende Rechtsgrundlage, wenn besondere Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1DSGVO verarbeitet werden. Sofern Account-Inhaberinnen sensible Daten öffentlich teilen, ist deren Verarbeitung nach Art. 9 Abs. 2 e) DSGVO erlaubt. Einige der Daten werden jedoch von Account-Inhaberinnen nicht „offensichtlich öffentlich gemacht“. Das betrifft insbesondere solche Beiträge, die nur für Followerinnen oder erwähnte Profile sichtbar sind. Ein Problem besteht aber auch dann, wenn Account-Inhaberinnen bei Umfragen antworten, die sensible Themen betreffen.

---

248 Artt. 44, 49 Abs. 1 b) DSGVO.
249 Vgl. EuGH, Urteil vom 6. November 2003 – C-101/01 –, juris, Rn. 69 f.
250 Vgl. https://blog.riemann.cc/projects/mastodon-privacy-policy-generator/.

Die Verarbeitung dieser freiwillig angegebenen Informationen kann insofern nur auf eine Einwilligung nach Art. 6 Abs. 1 a), 9 Abs. 2 a) DSGVO gestützt werden. Wenn Account-Inhaberinnen solche Informationen mitteilen, ist davon auszugehen, dass sie mit einer „eindeutig bestätigenden Handlung“ in die hierfür technisch notwendigen Verarbeitungsvorgänge einwilligen. Diese Vorgänge erfolgen zu einem eng umgrenzten Zweck und sind auch notwendig, damit Instanzbetreiberinnen ihre Pflicht aus dem Nutzungsvertrag erfüllen können.[251] Auch wenn Account-Inhaberinnen die Informationen nicht „veröffentlichen“, ist hier von einer bewussten, selbstbestimmten und aktiven Handlung auszugehen. Die Account-Inhaberinnen klicken in dem Moment aktiv auf "Veröffentlichen" und haben ihre Beitrag und die gewählten Privatsphäreneinstellungen dabei unmittelbar vor Augen. Instanzbetreiberinnen stehen allerdings vor dem Problem, dass sie eine solche Einwilligung nicht dokumentieren können. Insofern können sich für Instanzbetreiberinnen Beweisschwierigkeiten ergeben, dass tatsächlich eine Einwilligung erteilt wurde.[252] Sie können allerdings darlegen, dass ein Beitrag versendet wurde und welche Software zu diesem Zeitpunkt eingesetzt wurde.

7.3 Informations- und Auskunftsrechte

Die Informationspflichten gegenüber Account-Inhaberinnen aus Art. 13 DSGVO stellen die meisten Instanzbetreiberinnen ebenfalls vor Herausforderungen.

Gemäß Art. 13 Abs. 1 e) DSGVO müssen Instanzbetreiberinnen gegebenenfalls über Empfängerinnen oder Kategorien von Empfängerinnen informieren. Empfängerinnen sind insbesondere Account-Inhaberinnen und Betreiberinnen anderer Instanzen, die der betroffenen Account-Inhaberin folgen oder einer Person folgen, die den Beitrag „geboostet“ hat (siehe 2.3). In der Administrationsoberfläche können Instanzbetreiberinnen die bekannten Instanzen einsehen. Es stellt sich die Frage, ob diese Liste eigentlich auch den Account-Inhaberinnen zugänglich gemacht werden müsste. Art. 13 Abs. 1 e) DSGVO lässt es ausdrücklich genügen, dass die Kategorien von Empfängerinnen genannt werden. Es genügt daher, abstrakt zu beschreiben, an welche anderen Instanzen die Beiträge übermittelt werden.[253] Grundsätzlich können Account-

251 Vgl. EuGH, Urteil vom 4. Juli 2023 – C-252/21 –, Rn. 145, 149, juris.

252 Siehe *Freund*, in: Schuster/Grützmacher (Hrsg.), IT-Recht, 1. Aufl. 2020, a) Ausdrückliche Einwilligung (Art. 9 Abs. 2 Buchst. a), Rn. 14; Jaspers/Mühlenbeck/Schwartmann in: Schwartmann/Jaspers/Thüsing/ Kugelmann (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2020, Artikel 9 Verarbeitung besonderer Kategorien personenbezogener Daten, Rn. 125; *Korge*, in: Gierschmann (Hrsg.), Kommentar Datenschutz-Grundverordnung, 1. Aufl. 2018, Article 9/Artikel 9, Rn. 20.

253 Siehe *Franck*, in: Gola/Heckmann, DS-GVO – BDSG, 3. Aufl. 2022, DS-GVO Art. 13 Rn. 20.

Inhaberinnen dies schon anhand ihrer Followerinnen erkennen. Die Funktionsweise des Fediverse sollte in den Datenschutzhinweisen möglichst prägnant beschrieben sein. Zu empfehlen ist auch, dort gegebenenfalls eingebundene Relays zu erwähnen.

Die Auskunftspflichten nach Art. 15 DSGVO haben keine darüber hinausgehende Bedeutung. Es ist davon auszugehen, dass Account-Inhaberinnen wissen, dass sie sich auf der Fediverse-Instanz registriert haben und somit personenbezogene Daten von ihnen verarbeitet werden. Die in Art. 15 DSGVO genannten Punkte müssen schließlich auch gemäß Art. 13 DSGVO in den Datenschutzhinweisen enthalten sein.

7.4 Recht auf Löschung

Instanzbetreiberinnen sind verpflichtet, auf Verlangen der Account-Inhaberinnen die sie betreffenden personenbezogenen Daten zu löschen. Die von Account-Inhaberinnen veröffentlichten Beiträge oder auch Profilinformationen können ohne Weiteres selbst von den Account-Inhaberinnen gelöscht werden. Damit werden diese Beiträge auch aus der Datenbank des Servers gelöscht.[254]

Fraglich ist, ob Instanzbetreiberinnen nach Art. 17 Abs. 2 DSGVO dazu verpflichtet sind, Löschanfragen an andere Instanzen weiterzuleiten, welche über eine Kopie des Beitrags oder der Profilinformationen verfügen. Schließlich wurden diese Informationen gerade nicht durch die Instanzbetreiberin öffentlich gemacht, sondern durch die Account-Inhaberin selbst. Instanzbetreiberinnen erfüllen diese Pflicht jedenfalls, indem sie das Löschen eines Beitrags oder die Aktualisierung der Profilinformationen an alle empfangenden Instanzen weiterleiten. Im Rahmen von Art. 17 Abs. 2 DSGVO ist es gerade nicht erforderlich, dass die Informationen auf anderen Instanzen tatsächlich gelöscht werden.[255] Es ist schließlich möglich, dass Löschanfragen von anderen Instanzen nicht umgesetzt werden, auch weil es zwischen verschiedener Software zu Kompatibilitätsproblemen kommen kann.

Account-Inhaberinnen können auch ihren Account über die Benutzerüberfläche löschen, nicht jedoch den Account-Namen selbst.[256] Das ist aus Sicherheitsgründen nachvollziehbar, da es

254 https://docs.joinmastodon.org/spec/activitypub/.
255 Siehe Nolte/Werkmeister, in: Gola/Heckmann, DSGVO – BDSG, 3. Aufl. 2022 Art. 17 DSGVO Rn. 41.
256 Siehe https://docs.joinmastodon.org/user/moving/#delete.

ansonsten anderen Personen möglich wäre, diese Identität zu „stehlen“. Insofern lässt sich argumentieren, dass die Speicherung weiterhin notwendig ist, um nachvertragliche Schutzpflichten gegenüber Account-Inhaberinnen zu erfüllen. Möglicherweise ist deshalb auch das Recht auf Löschung gemäß Art. 17 Abs. 1 a) DSGVO eingeschränkt. Rein technisch ist es aber möglich, einen Account-Namen aus der Datenbank zu löschen. Das wird jedenfalls auf Verlangen der (ehemaligen) Account-Inhaberinnen erforderlich sein.

7.5 Recht auf Datenübertragbarkeit

Art. 20 DSGVO gibt Account-Inhaberinnen das Recht, die von ihnen bereitgestellten personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und einem anderen Verantwortlichen zu übermitteln. Account-Inhaberinnen haben die Möglichkeit, alle sieben Tage eine Archivdatei aller ihrer hochgeladenen Beiträge und Medien zu erhalten. Daneben können sie CSV-Dateien mit Listen der Accounts, denen sie folgen, ihre manuell konfigurierten Listen, Blocklisten, Stummschaltlisten und Lesezeichen herunterladen. Diese CSV-Dateien können auf einer anderen Instanz problemlos importiert werden.

Es gibt außerdem die Möglichkeit, auf eine andere Mastodon-Instanz umzuziehen und die Followerinnen automatisiert zu übertragen. Eine solche automatisierte Übermittlung ist überhaupt nur von Art. 20 DSGVO gefordert, soweit sie technisch möglich ist.

Die von Account-Inhaberinnen hochgeladenen Beiträge können nicht ohne Weiteres auf anderen Instanzen importiert werden. Der Import der übermittelten Daten ist jedoch von Art. 20 DSGVO gar nicht vorgesehen.

8. Pflichten gegenüber Account-Inhaberinnen anderer Instanzen

Wie unter 2.3 beschrieben, werden die von Account-Inhaberinnen geteilten Profilinformationen und Beiträge nicht nur auf der eigenen Instanz veröffentlicht, sondern auch an föderierende Instanzen übermittelt. Eine Instanzbetreiberin verarbeitet also nicht nur Daten der Personen, die auf der eigenen Instanz einen Account haben, sondern auch Daten von Account-Inhaberinnen anderer Instanzen.

8.1 Anwendbarkeit von DSGVO und TDDDG

Auch die direkten Beiträge, die Account-Inhaberinnen von den Nutzerinnen anderer Instanzen erhalten, dürften dem Fernmeldegeheimnis unterliegen (siehe 5.2.3). Im Übrigen ist die DSGVO anwendbar.

8.2 Rechtsgrundlagen für die Datenverarbeitung

Die Verarbeitung von öffentlichen Beiträgen ist nach Art. 6 Abs. 1 f) DSGVO zulässig. Instanzbetreiberinnen haben ein berechtigtes Interesse daran, die Beiträge anderer Instanzen zu replizieren.[257] Andernfalls könnten auf der Instanz ausschließlich die Beiträge der eigenen Instanz angezeigt werden. Theoretisch ist es zwar möglich, eine Fediverse-Instanz als Intranet zu betreiben und mit keiner anderen Instanz zu föderieren. Das würde aber gerade der Idee des Fediverse zuwiderlaufen.

Dem Interesse anderer Instanzbetreiberinnen steht ein eher theoretisches Interesse der jeweiligen Account-Inhaberin entgegen. Denkbar ist zum Beispiel, dass sich Personen auf der Instanz registrieren, die nicht wissen, wie das Fediverse oder Mastodon funktioniert. In aller Regel entspricht es aber gerade dem Interesse von Account-Inhaberinnen, mit den Account-Inhaberinnen anderer Instanzen interagieren zu können. Andernfalls wäre es erforderlich, auf zahlreichen Instanzen zusätzliche Accounts anzulegen und somit mehreren Personen die

257 Siehe auch die Datenschutzerklärung von freiburg.social, https://freiburg.social/privacy-policy.

Bestandsdaten preiszugeben. Die Föderation mit anderen Instanzen ist vielmehr ein Grund dafür, dass sich die Account-Inhaberinnen für einen Fediverse-Account entschieden haben. Es entspricht also den Erwartungen der Account-Inhaberinnen, dass Inhalte auch von anderen Instanzen aus abrufbar sind, was technisch-notwendig eine Speicherung auf anderen Servern erfordert.[258]

Auch insofern ergeben sich jedoch Probleme, wenn die Account-Inhaberinnen anderer Instanzen sensible Informationen im Sinne des Art. 9 Abs. 1 DSGVO teilen. Öffentliche Beiträge und Profilinformationen werden zwar nach Art. 9 Abs. 2 e) DSGVO von den Betroffenen offensichtlich öffentlich gemacht. Das gilt jedoch nicht für die Beiträge, die nur für Followerinnen oder erwähnte Profile sichtbar sind.

Es ist aber auch hier von einer Einwilligung auszugehen, da auch die Account-Inhaberinnen anderer Instanzen diese Informationen mit einer „eindeutig bestätigenden Handlung" teilen (siehe 7.2.4).

8.3 Informations- und Auskunftsrechte

Auch die Zwecke und die Rechtsgrundlage einer Speicherung dieser Inhalte von Account-Inhaberinnen anderer Instanzen müssen sich in den Datenschutzhinweisen wiederfinden. Soweit die Verarbeitung auf ein berechtigtes Interesse der Instanzbetreiberinnen gestützt wird, ist dieses gemäß Art. 13 Abs. 1 d) bzw. Art. 14 Abs. 2 b) DSGVO zu begründen.

Wer einen Fediverse-Account besitzt, kann von den Betreiberinnen anderer Instanzen Auskunft darüber verlangen, ob eigene personenbezogene Daten verarbeitet werden. Als Instanzbetreiberin ist es nicht nur möglich einzusehen, welche Instanzen die „eigenen" Beiträge empfangen, sondern auch von welchen anderen Instanzen die eigene Instanz Beiträge erhält. Instanzbetreiberinnen können einer anfragenden Person also grundsätzlich Auskunft darüber geben, ob ihre Daten potenziell verarbeitet werden. Eine weitergehende Auskunft ist hingegen schwieriger umsetzbar und erfordert eine aufwändigere Suche in der eigenen Datenbank.

258 Vgl. EuGH, Urteil vom 4. Juli 2023 – C-252/21 –, Rn. 116, juris.

8.4 Recht auf Löschung und Widerspruchsrecht

Da die Verarbeitung von Beiträgen anderer Instanzen auf das berechtigte Interesse der Instanzbetreiberin gestützt wird, können die betroffenen Account-Inhaberinnen hiergegen Widerspruch nach Art. 21 Abs. 1 DSGVO einlegen. Instanzbetreiberinnen müssen in diesem Fall die Verarbeitung einstellen oder überwiegende schutzwürdige Interessen nachweisen. Ein solches Interesse kann darin bestehen, dass die betroffene Account-Inhaberin den Beitrag auf der Originalinstanz noch nicht gelöscht hat.

Sofern der Originalbeitrag hingegen gelöscht wurde, fällt die Interessenabwägung zulasten der Instanzbetreiberin aus. In der Regel werden Löschanfragen automatisch von der Originalinstanz weitergeleitet und umgesetzt, sodass es unwahrscheinlich ist, dass Instanzbetreiberinnen überhaupt einen Widerspruch oder eine Löschanfrage von Account-Inhaberinnen anderer Instanzen erhalten. Aber gerade bei der Kommunikation zwischen unterschiedlicher Software erfolgt das Löschen über Instanzen hinweg oft nicht fehlerfrei. Ein weiteres Problem ergibt sich dann, wenn eine Instanz abgeschaltet wurde, ohne dass zuvor alle Beiträge gelöscht wurden. Für ehemalige Account-Inhaberinnen ist es in diesem Fall sehr schwierig herauszufinden, auf welchen Instanzen noch Kopien ihrer alten Beiträge liegen. Das „Recht auf Vergessenwerden“ ist aufgrund dieser Problematik im Internet allgemein schwer durchzusetzen.

Hinzu kommt, dass Löschanfragen bezüglich der Inhalte anderer Instanzen für Instanzbetreiberinnen schwer umsetzbar sind. Theoretisch wäre es möglich, den zu löschenden Beitrag mittels einer SQL-Anfrage aus der Datenbank zu löschen. Es wäre wünschenswert, wenn es hierfür in der Software eine einfachere und weniger fehleranfällige Lösung gäbe.

Die Ausübung des Rechts auf Löschung kommt im Wesentlichen der Ausübung des Widerspruchsrechts nach Art. 21 DSGVO gleich. Sofern der Beitrag, auf den sich die Löschanfrage oder der Widerspruch bezieht, auf der Originalinstanz gelöscht ist, haben Instanzbetreiberinnen jedenfalls kein berechtigtes Interesse daran, diese Beiträge weiter zu speichern.

9. Pflichten gegenüber sonstigen Dritten

Sonstige Personen können betroffen sein, wenn Account-Inhaberinnen beispielsweise Informationen über Dritte veröffentlichen. Denkbar ist auch, dass Dritte die Instanzbetreiberin per E-Mail kontaktieren oder ihre Rechte aus der DSGVO geltend machen.

9.1 Anwendbarkeit der DSGVO

Sofern personenbezogene Daten Dritter über eine Mastodon-Instanz veröffentlicht werden, ist die DSGVO anwendbar. Auch aus Sicht von (privaten) Account-Inhaberinnen greift hier die Haushaltsausnahme nicht ein. Die von der DSGVO nicht erfassten persönlichen oder familiären Tätigkeiten sind sozusagen „öffentlichkeitsfeindlich".[259] Das bedeutet, dass die Haushaltsausnahme nicht gilt, wenn die personenbezogenen Daten auf einer Internetseite veröffentlicht und somit einer unbegrenzten Zahl von Personen zugänglich gemacht werden. Da ein Social-Media-Profil heutzutage oft als Ersatz für eine eigene Webseite angelegt wird, gelten diese Überlegungen auch für Inhaberinnen von Mastodon-Accounts. Es wird aber auch die Ansicht vertreten, dass die Nutzung von sozialen Netzwerken durch Privatpersonen generell vom Anwendungsbereich der DSGVO ausgeschlossen sein soll, wie es vom Erwägungsgrund 18 der DSGVO nahegelegt wird.[260]

Unabhängig von diesem Meinungsstreit bleibt die Verantwortlichkeit von Instanzbetreiberinnen jedenfalls bestehen. Schließlich soll die Haushaltsausnahme nach dem Erwägungsgrund 18 ausdrücklich nicht für die Verantwortlichen gelten, die die Instrumente für die Verarbeitung personenbezogener Daten bereitstellen.

Die DSGVO ist in der Regel auch dann anwendbar, wenn Personen die Instanzbetreiberin per E-Mail kontaktieren.

---

259 EuGH, Urteil vom 6. November 2003 – C-101/01 –, juris (Rn. 47); *Ernst*, in: Paal/Pauly (Hrsg.), DS-GVO BDSG, 3. Aufl. 2021, DS-GVO Art. 2 Rn. 21.

260 So etwa *Bäcker*, in: Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, 43. Edition, 01.11.2021, DS-GVO Art. 2 Rn. 21.

9.2 Rechtsgrundlagen für die Datenverarbeitung

Das Veröffentlichen von personenbezogenen Daten Dritter kann in bestimmten Fällen durch die Meinungsfreiheit der Account-Inhaberinnen gerechtfertigt sein. Das Interesse der Account-Inhaberinnen muss im Rahmen von Art. 6 Abs. 1 f) DSGVO aber immer im Einzelfall mit den Interessen und Grundrechten der betroffenen Person abgewogen werden. Um ihrer Verantwortlichkeit gerecht zu werden, sollten Instanzbetreiberinnen den Account-Inhaberinnen untersagen, Beiträge zu veröffentlichen, die Informationen über Dritte beinhalten und nicht von der Meinungsfreiheit gedeckt sind. Sofern Instanzbetreiberinnen von solchen Beiträgen Kenntnis erlangen, sollten diese gelöscht werden. Dies gilt insbesondere im Falle von Doxxing.

Es darf sich grundsätzlich nicht um besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO handeln. Nur im Ausnahmefall sind solche Beiträge zulässig, zum Beispiel weil die Dritte eingewilligt hat oder die Informationen selbst offensichtlich öffentlich gemacht.[261]

Wenn sich Personen per E-Mail an die Instanzbetreiberin wenden, verarbeitet diese deren E-Mail-Adresse sowie Nachrichteninhalte. Diese Datenverarbeitungen sind, im Rahmen des Erforderlichen, vom berechtigten Interesse der Instanzbetreiberin nach Art. 6 Abs. 1 f) DSGVO gedeckt.

9.3 Informations- und Auskunftspflichten

Wenn Account-Inhaberinnen personenbezogene oder personenbeziehbare Informationen über Dritte veröffentlichen, müssten diese eigentlich nach Art. 13 oder 14 DSGVO informiert werden. In sozialen Medien werden allerdings ständig – meist auch berechtigterweise – Informationen über Dritte geteilt, insbesondere über Personen des öffentlichen Lebens. Es wäre für Instanzbetreiberinnen mit einem unverhältnismäßigen Aufwand verbunden, die betroffenen Personen in sämtlichen dieser Fälle zu kontaktieren. Daher ist die Informationspflicht nach Art. 14 Abs. 5 DSGVO (analog) ausgeschlossen.

261 Art. 9 Abs. 2 a) und e) DSGVO.

Auch Auskunftspflichten nach Art. 15 DSGVO können Instanzbetreiberinnen vor Herausforderungen stellen. Instanzbetreiberinnen können zumindest versuchen, über eine Datenbankabfrage zu ermitteln, ob Informationen über die betroffene Person geteilt wurden.

9.4 Recht auf Löschung und Widerrufsrecht

Löschanfragen können grundsätzlich auch an die jeweilige Account-Inhaberin oder die Instanzbetreiberin gerichtet werden. Auf eine entsprechende Anfrage hin können aber auch Instanzbetreiberinnen verpflichtet sein, einen Beitrag zu löschen.

Auch in dem Fall, dass Account-Inhaberinnen Informationen über Dritte veröffentlichen, kommt eine Pflicht zur Weiterleitung der Löschanfrage nach Art. 17 Abs. 2 DSGVO nicht in Betracht. Schließlich wurden diese Informationen nicht durch die Instanzbetreiberin öffentlich gemacht, sondern durch die Account-Inhaberin. Sofern Instanzbetreiberinnen diese Informationen selbst öffentlich gemacht haben, ist das automatisierte Weiterleiten der Löschanfrage an föderierende Instanzen aber als ausreichend zu betrachten. Es wäre in dem Fall ratsam, auch stichprobenartig zu kontrollieren, ob die Löschanfrage von anderen Instanzen umgesetzt wurde.

Auch E-Mails, die Instanzbetreiberinnen erreichen, sind zu löschen, sobald das Anliegen der kontaktierenden Person erledigt ist. Die Pflicht zur Löschung kann aber beispielsweise ausgeschlossen sein, wenn die Instanzbetreiberin die E-Mail benötigt, um rechtliche Ansprüche geltend zu machen oder sich gegen solche zu verteidigen.[262]

262 Art. 17 Abs. 3 DSGVO.

10. Organisatorische Pflichten und „Schwellwertanalyse“

Die organisatorischen Pflichten der Verantwortlichen werden vor allem im praktischen Teil dieses Leitfadens[263] dargestellt.

Die nach den Art. 24, 25 32 DSGVO nötigen technischen und organisatorischen Maßnahmen sowie datenschutzfreundlichen Voreinstellungen werden in dem Dokument „Datenschutzfreundliche Konfiguration“ erläutert.

Weitere organisatorische Pflichten sind Bestandteil des Dokuments „Praktische Umsetzung und Musterdokumente“. Dazu gehört insbesondere das Erstellen eines Verzeichnisses für Verarbeitungstätigkeiten nach Art. 30 DSGVO, wofür der Leitfaden auch ein Muster enthält[264]. Unter „Praktische Umsetzung und Musterdokumente“ finden sich auch Ausführungen dazu, wann eine Datenschutzbeauftragte zu benennen ist. Zudem werden dort weitere Dokumentationspflichten beschrieben, die der Erfüllung der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO dienen.

Weitergehender Klärungsbedarf ergibt sich allerdings dahingehend, ob Instanzbetreiberinnen nach Art. 35 DSGVO eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen haben. Das ist dann der Fall, wenn eine Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Die Prüfung, ob eine DSFA erforderlich ist, wird als „Schwellwertanalyse“ bezeichnet. Das Ergebnis der Schwellwertanalyse sollte im Verzeichnis der Verarbeitungstätigkeiten oder gesondert dokumentiert werden.

Das Ziel einer DSFA ist es, konkrete Risiken für Betroffene und Maßnahmen zur Eindämmung zu identifizieren. Eine solche DSFA muss schon vor Beginn der Datenverarbeitung erfolgen, also bevor eine Instanz in Betrieb genommen wird. Zudem sollte eine solche Datenschutz-Folgenabschätzung regelmäßig überprüft und gegebenenfalls überarbeitet werden.

263 https://sds-links.de/mastodon-leitfaden.
264 https://sds-links.de/mastodon-muster-vvt.

Grundsätzlich ist es immer sinnvoll, vor Inbetriebnahme einer Fediverse-Instanz eine DSFA durchzuführen. Eine Hilfestellung für das Verfahren bieten insbesondere die Leitlinien der Artikel-29-Datenschutzgruppe zur DSFA, welche vom Europäischen Datenschutzausschuss übernommen wurden (Working Paper 248),[265] sowie das Standard-Datenschutzmodell der Datenschutzkonferenz.[266] Gerade für ehrenamtliche Instanzbetreiberinnen stellt die Durchführung einer DSFA dennoch eine Herausforderung dar. So heißt es auch im Kurzpapier Nr. 5 der Datenschutzkonferenz, eine DSFA könne im Allgemeinen nur von einem interdisziplinären Team erstellt werden, das Kompetenzen im Bereich Datenschutz, Risikoermittlung und Fachprozesse mitbringt.[267] Für Instanzbetreiberinnen stellt sich daher die Frage, ob eine Datenschutz-Folgenabschätzung rechtlich vorgeschrieben ist. Die Antwort hierauf kann je nach Instanz unterschiedlich ausfallen.

10.1 Risikoprognose

Der Betrieb einer Fediverse-Instanz ist stets mit Risiken verbunden. Ein Risiko für betroffene Personen ist immer dann gegeben, wenn die Möglichkeit besteht, dass ein Schaden eintritt, oder ein mögliches Ereignis zu weiteren Schäden führen kann.[268] Es müssen also auch solche Situationen betrachtet werden, in denen etwas „schiefgegangen" ist.[269] Ob ein hohes Risiko wahrscheinlich ist, ist zum einen nach der *Schwere* des Schadens und zum anderen nach der *Wahrscheinlichkeit* des Schadenseintritts zu beurteilen.[270] Ein hohes Risiko für Betroffene kann sich aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung ergeben. Unter solchen hohen Risiken sind *erhebliche* wirtschaftliche oder gesellschaftliche Nachteile zu verstehen.[271] Sie können in einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanzieller Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten oder in der unbefugten Aufhebung der Pseudonymisierung bestehen.

---

265 Datenschutzgruppe nach Artikel 29, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", Working Paper 248 Rev. 01, zuletzt überarbeitet und angenommen am 4. Oktober 2017.
266 AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Hrsg.), Das Standard-Datenschutzmodell. Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, Version 2.0.
267 Datenschutzkonferenz, Kurzpapier Nr. 5. Datenschutz-Folgenabschätzung nach Art. 35 DSGVO, S. 2.
268 Datenschutzkonferenz, Kurzpapier Nr. 18. Risiko für die Rechte und Freiheiten betroffener Personen, S. 1.
269 Vgl. Datenschutzkonferenz, Kurzpapier Nr. 18. Risiko für die Rechte und Freiheiten betroffener Personen, S. 2.
270 Vgl. Datenschutzkonferenz, Kurzpapier Nr. 18. Risiko für die Rechte und Freiheiten betroffener Personen, S. 4.
271 Siehe Erwägungsgrund 75 der DSGVO.

Im Fediverse sind solche Risiken vor allem dann zu befürchten, wenn weitere Verarbeitungsvorgänge hinzukommen, zum Beispiel wenn Instanzbetreiberinnen oder Dritte Daten verwenden, um Persönlichkeitsprofile der Account-Inhaberinnen zu erstellen. Denkbar sind aber auch Fälle, in denen unbefugte Personen Zugang zu den Daten erhalten oder Instanzen ohne Ankündigung abgeschaltet werden. Außerdem besteht das Risiko, dass die Account-Inhaberinnen unerlaubt persönliche Daten Dritter offenlegen.

10.2 Besonders riskante Verarbeitungstätigkeiten

Art. 35 Abs. 3 DSGVO nennt beispielhaft einige Verarbeitungsvorgänge, für die zwingend eine DSFA durchzuführen ist. Bei Fediverse-Instanzen kommt insbesondere die in Buchst. b genannte „umfangreiche Verarbeitung besonderer Kategorien von personenbezogener Daten gemäß Art. 9 Absatz 1“ in Betracht.

Sensible Daten im Sinne des Art. 9 Abs. 1 DSGVO werden auf nahezu allen, das heißt auch auf thematisch offenen, Instanzen verarbeitet. Wie auf allen sozialen Medien finden auch im Fediverse politische Diskussionen statt. Aus entsprechenden Beiträgen können daher insbesondere politische Meinungen sowie religiöse oder weltanschauliche Überzeugungen hervorgehen. Aber auch Inhalte, aus denen die ethnische Herkunft hervorgeht, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung sind vom Schutz des Art. 9 DSGVO erfasst. Jedoch liefert der Erwägungsgrund 91 S. 2 der DSGVO einen Anhaltspunkt dafür, dass es beispielsweise um solche Verarbeitungsvorgänge gehen soll, bei denen Verantwortliche auf Grundlage solcher Daten Entscheidungen in Bezug auf betroffene Personen treffen. Auch Datenverarbeitungen im Zusammenhang mit Führungszeugnissen und Sicherheitsüberprüfungen werden in der Kommentarliteratur als Beispiel genannt.[272] Ein vergleichbar hohes Risiko ergibt sich demgegenüber nicht aus jeglicher Verarbeitung sensibler Daten nach Art. 9 Abs. 1 DSGVO. Entscheidend ist zum Beispiel auch, ob eine nach dem Stand der Technik neue Technologie eingesetzt wird oder die Verarbeitungsvorgänge es Betroffenen erschweren, ihre Rechte wahrzunehmen. In Hinblick auf das Fediverse ist auch zu berücksichtigen, dass solche Daten in der Regel auf Veranlassung der Account-Inhaberinnen

272 *Ferik*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG, Artikel 35 Datenschutz-Folgenabschätzung, Rn. 45.

verarbeitet werden, und zwar zu einem eng begrenzten Zweck. Andererseits ist die Nutzung von sozialen Medien immer mit Risiken verbunden.

10.3 „Muss-Liste“

Die Aufsichtsbehörden führen nach Art. 35 Abs. 4 DSGVO Listen mit Verarbeitungsvorgängen, für die auf jeden Fall eine DSFA durchzuführen ist. Zu den dort genannten Verarbeitungen gehört unter anderem die Erstellung umfassender Profile über die Interessen, das Netz persönlicher Beziehungen oder die Persönlichkeit der Betroffenen. Als typisches Einsatzfeld derartiger Verarbeitungsvorgänge wird der Betrieb von großen sozialen Netzwerken genannt. Das ist allerdings nicht so zu verstehen, dass für den Betrieb eines großen sozialen Netzwerks immer eine DSFA durchzuführen wäre. Die großen, proprietären sozialen Netzwerke erstellen üblicherweise Persönlichkeitsprofile, um etwa möglichst passende Kontaktvorschläge zu generieren. Das ist bei Fediverse-Instanzen in der Regel gerade nicht der Fall. Die „Muss-Liste“ ist zwar nicht abschließend, bietet jedoch einen Anhaltspunkt dafür, dass der Betrieb eines sozialen Netzwerkes allein noch nicht zur Durchführung einer DSFA verpflichtet.

10.4 Kriterien im Working Paper 248

Im Working Paper 248 werden neun Kriterien genannt, die für die Schwellwert-Analyse herangezogen werden müssen. Sind mindestens zwei der Kriterien erfüllt, ist zumeist eine DSFA durchzuführen. Das ergibt sich jedoch nicht zwingend. Umgekehrt kann eine DSFA auch erforderlich sein, wenn nur eines der Kriterien erfüllt ist. Letztlich kommt es also allein auf die Prognose an, ob die Verarbeitungsvorgänge einer konkreten Fediverse-Instanz wahrscheinlich ein hohes Risiko mit sich bringen.

10.4.1 Bewerten oder Einstufen

Ein Kriterium ist das Erstellen von Profilen und Prognosen, und zwar insbesondere auf der Grundlage von Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel der betroffenen Person.[273] Auch bei Mastodon ist es inzwischen möglich, im Menü „Entdecken“ besonders

273 Erwägungsgründe 71 und 91 der DSGVO.

beliebte Beiträge, Hashtags oder Profile zu entdecken. Diese Vorschläge sind jedoch nicht personalisiert, beruhen also nicht etwa auf Analysen der persönlichen Vorlieben, Interessen oder des Verhaltens von Account-Inhaberinnen. Die Mastodon gGmbH wirbt gerade damit, dass es auf Mastodon keine Algorithmen gibt, sondern die Beiträge in chronologischer Reihenfolge angezeigt werden.[274] Dennoch gibt es bereits Projekte und Clients, die das Fediverse um personalisierte Algorithmen erweitern oder Analyse-Tools für Nutzerinnen anbieten.[275]

10.4.2 Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung

Ein weiteres Kriterium ist, ob auf Grundlage der Datenverarbeitung Entscheidungen getroffen werden sollen, welche Rechtswirkung gegenüber betroffenen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen.[276] Wenn Account-Inhaberinnen private Informationen über sich selbst in sozialen Netzwerken veröffentlichen, kann das durchaus negative Auswirkungen zur Folge haben und in Extremfällen beispielsweise „den Job kosten". Die Selbstdarstellung im Internet kann sich zum Beispiel negativ auf ein Bewerbungsverfahren auswirken oder, je nach Äußerung, sogar eine Kündigung zur Folge haben. Solche Entscheidungen mit Rechtswirkung sind jedoch eine zufällige Folge dieser Verarbeitungsvorgänge. Die Instanzbetreiberinnen verarbeiten diese Daten lediglich, um den Account-Inhaberinnen den Dienst zu Verfügung zu stellen und nicht zu dem Zweck, dass solche Entscheidungen getroffen werden.

10.4.3 Systematische Überwachung

Auch die systematische Überwachung Betroffener ist ein Kriterium. Damit sind Verarbeitungsvorgänge gemeint, die die Beobachtung, Überwachung oder Kontrolle von Betroffenen zum Ziel haben. Wie unter 2.2.1 und 2.3 beschrieben, aggregiert eine Mastodon-Instanz die Beiträge von allen Account-Inhaberinnen, denen eine Account-Inhaberin der eigenen Instanz folgt. Hierin ist jedoch noch keine systematische Überwachung zu sehen. In vielen Fällen wird es Instanzbetreiberinnen schon gar nicht möglich sein, alle Inhalte zur Kenntnis zu nehmen.

---

274 Siehe https://joinmastodon.org/.
275 Siehe https://getmammoth.app/ oder https://fedica.com/social-media/mastodon.
276 Art. 35 Abs. 3 lit. a DSGVO.

10.4.4 Vertrauliche Daten oder höchst persönliche Daten

Ein weiteres Kriterium ist die Verarbeitung vertraulicher Daten oder höchst persönlicher Daten, welche über die von Art. 9 Abs. 1 DSGVO erfassten Daten hinausgehen können. Als vertraulich gilt hier etwa auch die elektronische Kommunikation. Da im Fediverse durchaus auch privat über „direkte Beiträge“ kommuniziert wird, dürfte jedenfalls dieses eine Kriterium erfüllt sein.

10.4.5 Datenverarbeitung in großem Umfang

Als „umfangreich“ sollen nach Erwägungsgrund 91 der DSGVO solche Verarbeitungsvorgänge gelten, die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten oder eine große Zahl von Personen betreffen. Über die hier maßgeblichen Schwellenwerte kann nur spekuliert werden. Entscheidend dürfte sein, ob flächendeckend Daten in einem größeren geografischen Ausmaß verarbeitet werden.[277] Ein Beispiel wäre eine Fediverse-Instanz für eine Stadt, auf der nahezu alle Bewohnerinnen der Stadt vertreten sind. Die Anzahl der Account-Inhaberinnen ist aber auch bei größeren Fediverse-Instanzen noch weit von der „sehr großer Online-Plattform“ im Sinne des DSA entfernt. Eine Verarbeitung soll zudem nicht umfangreich sein, wenn sensible Daten von einem einzelnen Arzt, einzelnen Angehörigen eines Gesundheitsberufes oder einem einzelnen Rechtsanwalt vorgenommen wird. Der Hintergrund dieser Erwägungen ist unklar. Hieraus lässt sich aber möglicherweise schließen, dass Verarbeitungsvorgänge durch einzelne Personen, etwa durch einzelne Instanzbetreiberinnen, nicht erfasst sein sollen.

10.4.6 Abgleichen oder Zusammenführen von Datensätzen

Ein Kriterium ist zudem das Abgleichen oder Zusammenführen von Datensätzen, die beispielsweise aus zwei oder mehreren Datenverarbeitungsvorgängen stammen, welche zu unterschiedlichen Zwecken und/oder von verschiedenen Verantwortlichen durchgeführt werden. Es ließe sich daran denken, dass auch im Fediverse die Datensätze verschiedener Instanzen zusammengeführt werden. Jedoch ist das Kriterium nur erfüllt, wenn dieser Abgleich über die

277 Vgl. Datenschutzkonferenz, Kurzpapier Nr. 18. Risiko für die Rechte und Freiheiten betroffener Personen, S. 5.

vernünftigen Erwartungen der Betroffenen hinausgeht. Die Föderation der Instanzen im Fediverse dürfte hingegen gerade den Erwartungen der Account-Inhaberinnen entsprechen.

10.4.7 Daten zu schutzwürdigen Betroffenenen

Ein weiteres Kriterium ist die Verarbeitung von Daten zu schutzbedürftigen Betroffenen, beispielsweise Kindern oder psychisch Kranken. Hier kommt es darauf an, ob zwischen den Instanzbetreiberinnen und den Account-Inhaberinnen ein Machtungleichgewicht besteht. Selbst bei Instanzen, die auf Kinder ausgerichtet wird, wird jedoch nicht zwingend ein solches Machtungleichgewicht bestehen. Dies kann jedoch beispielsweise der Fall sein, wenn eine Lehrerin eine Fediverse-Instanz für eine Schulklasse betreibt.

10.4.8 Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen

Ein Kriterium ist schließlich auch die innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen. Ob es sich um neue Technologie handelt, ist nach dem aktuellen Stand der Technik zu beurteilen.[278] Für viele Account-Inhaberinnen mag Mastodon „neu“ sein, jedoch existiert das Fediverse schon seit ca. 15 Jahren und die zugrundeliegenden Technologien sind noch älter.

10.4.9 Fälle, in denen die Verarbeitung an sich „die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindert“

Die Verarbeitungsvorgänge im Fediverse dürften auch keine Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindern. Denkbar ist dies lediglich, wenn Profile und Beiträge gemeldet werden. Account-Inhaberinnen, die Regelverstöße begehen, kommt insoweit jedoch auch kein Nutzungsrecht an der Instanz zu.

278 Erwägungsgrund 91 der DSGVO.

11. Fazit

Als Ergebnis dieser juristischen Analyse lässt sich festhalten, dass der Betrieb einer Fediverse-Instanz rechtskonform gestaltet werden kann. Dabei gibt es einige Herausforderungen, insbesondere bei der Erfüllung von Informationspflichten. Die von Mastodon mitgelieferten Datenschutzhinweise sind unvollständig und müssen von Instanzbetreiberinnen angepasst werden. Besonders schwierig ist, die richtigen Rechtsgrundlagen für die Datenverarbeitungen zu finden.

Es verbleiben zudem einige rechtliche Unsicherheiten, die sich schon aus der Natur von sozialen Netzwerken ergeben. Soziale Netzwerke werden schließlich auch für die private Kommunikation und für den Austausch zu sensiblen Themen verwendet. Dass die damit verbundenen Rechtsfragen in der juristischen Fachliteratur kaum diskutiert werden, lässt sich nur damit erklären, dass zentralisierte und proprietäre soziale Netzwerke viel gravierendere Datenschutzverstöße begehen.

Im Vergleich mit „klassischen" sozialen Netzwerken zeigt sich, dass das Fediverse relativ datenschutzfreundlich konzipiert ist. Betreiberinnen von Mastodon-Instanzen sollten jedoch bestimmte Änderungen an der Konfiguration vornehmen. Insbesondere für die Speicherung von IP-Adressen gibt es nach der DSGVO keine Rechtsgrundlage.

Einige der Ausführungen in diesem Aufsatz bleiben mit einem Fragezeichen versehen. Das Fediverse und vor allem der Betrieb einer Mastodon-Instanz, werfen neue juristische Fragen auf, insbesondere in Bezug auf die (gemeinsame) Verantwortlichkeit der zahlreichen am Fediverse beteiligten Personen. Vor allem die Frage nach der gemeinsamen Verantwortlichkeit von Instanzbetreiberinnen hat an Brisanz gewonnen, seitdem Threads bereits einseitig mit dem Fediverse föderiert.[279] Im Fediverse sind die Verantwortungsbereiche allerdings klar abgegrenzt. Mastodon ist so konzipiert, dass den anderen Instanzbetreiberinnen grundsätzlich nicht vertraut wird.[280]

279 Siehe https://engineering.fb.com/2024/03/21/networking-traffic/threads-has-entered-the-fediverse/.
280 Siehe https://blog.joinmastodon.org/2023/07/what-to-know-about-threads/.

Als Schwierigkeit kommt hinzu, dass die relevanten Vorschriften noch nicht lange in Kraft sind und daher viele rechtliche Fragen ungeklärt sind. Der DSA trat erst im Februar 2024 in Kraft. Auch der Begriff des interpersonellen Kommunikationsdienstes ist relativ neu und erst wenig konturiert. Mit der Ablösung des TMG durch das DDG sind ebenfalls neue Unsicherheiten entstanden. Offen ist vor allem die Frage, ob Instanzbetreiberinnen für sämtliche Rechtsverletzungen von Dritten haften oder als „digitale Dienste“ von der Haftung privilegiert sind, wenn sie keine Kenntnis haben oder unverzüglich nach Kenntnis tätig werden.

Es zeigt sich, dass sich das Recht und seine Auslegung eher an proprietären, werbefinanzierten sozialen Netzwerken orientiert. Es lässt sich aber auch bei diesen sozialen Netzwerken ein Trend zur Dezentralisierung beobachten. Möglicherweise führt das in naher Zukunft zu mehr juristischen Diskussionen über föderalisierte soziale Netzwerke.

Bei dem Betrieb einer Fediverse-Instanz müssen bestimmte rechtliche Risiken in Kauf genommen werden. Ein Großteil dieser Risiken fällt weg, wenn die Instanz nur für den „Eigenbedarf“ oder für den Familien- und Freundeskreis betrieben wird. Wünschenswert wäre es daher, wenn der Betrieb einer eigenen Instanz noch mehr vereinfacht wird und nicht davon abhängt, dass Account-Inhaberinnen das nötige Kleingeld für einen Application Service Provider besitzen. Jedenfalls sollten Mastodon-Instanzen nicht zu groß werden, damit sich die personenbezogenen Daten nicht auf wenigen Instanzen konzentrieren.

Es bleibt zu hoffen, dass sich die Gemeinschaft der Instanzbetreiberinnen von den strengen Vorschriften nicht davon abhalten lässt, ihre Instanz weiter zu betreiben oder neu aufzusetzen. Eine weitere Hoffnung besteht darin, dass mit dem Wachstum des Fediverse und den Feststellungen in diesem Leitfaden auch der juristische Diskurs weiter angeregt wird. Hoffentlich wird so auch auch ohne gerichtliche Auseinandersetzungen mehr Rechtssicherheit für Instanzbetreiberinnen geschaffen.

Impressum

Herausgeberin
Stiftung Datenschutz
Karl-Rothe-Straße 10–14
04105 Leipzig
Telefon 0341 / 5861 555-0
Telefon 0341 / 5861 555-9
mail@stiftungdatenschutz.org
www.stiftungdatenschutz.org

STIFTUNG DATENSCHUTZ

Autorin
Rebecca Sieber
für die Stiftung Datenschutz

Idee und Projektleitung
Hendrik vom Lehn

Redaktionelle Bearbeitung
Theresa Wenzel

Version
V 1.1, Stand September 2024

Agenturpartner
KING CONSULT | Kommunikation

Die Arbeit der Stiftung Datenschutz wird aus dem Bundeshaushalt gefördert (Einzelplan des BMJ).

Bundesministerium der Justiz

Sofern nicht anders angegeben, sind alle Inhalte dieses Leitfadens unter der CC BY-ND 4.0-Lizenz veröffentlicht. Die Lizenzbedingungen sind unter https://creativecommons.org/licenses/by-nd/4.0/deed.de einsehbar.