STIFTUNG DATENSCHUTZ

Datenschutzrechtliche Fragestellungen beim Betrieb einer Mastodon-Instanz

Wissenschaftlicher Aufsatz

Autorin

Rebecca Sieber

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 Mastodon-Instanz

Inhaltsübersicht

1. Einleitung

1.1 Problemaufriss

Seit der Übernahme von Twitter durch Elon Musk sind die Augen zahlreicher Microbloggerinnen[1] auf Mastodon gerichtet. Auch die Tage von Reddit scheinen gezählt, was die Aufmerksamkeit auf Dienste wie Lemmy oder Kbin lenkt. 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, freie Verbünde von sozialen Netzwerken. Mastodon, oder das Fediverse, wird nicht von einem einzigen Unternehmen betrieben, sondern auch von zahlreichen Privatpersonen, Organisationen oder auch staatlichen Institutionen.[4] Finanziert wird der Betrieb einer Instanz meist durch Spenden oder aus der eigenen Tasche.

Während die einen das Ende des „Social Media-Zeitalters" voraussagen,[5] ist für andere das Fediverse der neue Hoffnungsträger. Das Fediverse verspricht mehr digitale Autonomie und gilt als datenschutzfreundliche Alternative.[6] Anders als Plattformen wie Instagram, Youtube oder TikTok werden Fediverse-Instanzen meist nicht profitorientiert betrieben. Die Software nutzt offene Protokolle, sodass Webseiten mit verschiedener Software über den Server hinaus kommunizieren können. Dadurch, dass es keinen zentralen Knotenpunkt im Fediverse gibt, wird eine effektive Überwachung der Accountinhaberinnen erschwert. Damit bieten sich beispielsweise auch weniger Geschäftsmodelle an, die auf personalisierter Werbung basieren. Fediverse-Instanzen sind keine „Walled Gardens"; sogar ein Umzug zu einer anderen Instanz ist möglich. Mastodon ist eine Freie Software, die auch auf einem eigenen Server betrieben werden kann. Das setzt allerdings technische Vorkenntnisse voraus, die nicht jede Person mitbringt. Ein

---

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. https://www.sueddeutsche.de/kultur/social-media-zukunft-essay-1.5695071.
6 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.

großer Teil registriert sich eher auf einigen wenigen, größeren Instanzen.[7] Dadurch kommen Hobby-Admins in die Verlegenheit, auch sensible Daten von Nutzerinnen aufzubewahren. Erst im Mai 2023 wurde eine unverschlüsselte Backup-Kopie einer Mastodon-Datenbank vom FBI beschlagnahmt, nachdem die aufbewahrende Person an einer Demonstration teilgenommen hatte.[8] Mit der Aufmerksamkeit, die vor allem Mastodon erhält, nehmen auch die Sorgen darüber zu, welche juristischen Angriffsflächen der Betrieb einer Fediverse-Instanz bietet. Es stellt sich auch 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.[9] Insofern existiert auch im Fediverse ein Spannungsfeld zwischen Selbstdarstellung, dem positiven Ausdruck informationeller Selbstbestimmung und der Gefährdung der Rechte und Freiheiten betroffener Personen.[10] 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.[11] Ein Risiko liegt darin, dass zwischenmenschliche Beziehungen offenbart werden. Hinzu kommt, dass Messengerfunktionen wie die direkten Beiträge bei Mastodon, 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, IP-Adressen sowie Antworten auf Umfragen aller Accountinhaberinnen der Instanz. Auch im Fediverse verbleiben also einige Risiken für die Rechte und Freiheiten betroffener Personen.

Für Gesetzgeber und Aufsichtsbehörden ist das Fediverse aufgrund seiner dezentralen Struktur schwer zu greifen. Bislang sind auch keine Sanktionen gegen Instanzbetreiberinnen bekannt. Ein Blick auf einschlägige Gesetze und Rechtsprechung macht deutlich, dass das Fediverse bisher nicht mitgedacht wurde. Dieser Aufsatz widmet sich den datenschutzrechtlichen

---

7 Siehe https://fediverse.observer/list. Nach dem Stand vom 26.06.2023 wurden 16 Fediverse-Instanzen mit je über 100.000 Accounts gezählt.
8 Siehe https://kolektiva.social/@admin/110637031574056150.
9 Dazu *Hornung*, Datenschutzrechtliche Aspekte der Social Media. In: Hornung/Müller-Terpitz (Hrsg.), Rechtshandbuch Social Media, 2. Aufl., Berlin 2021, S. 131 f.
10 Siehe auch *Hornung*, Datenschutzrechtliche Aspekte der Social Media. In: Hornung/Müller-Terpitz (Hrsg.), Rechtshandbuch Social Media, 2. Aufl., Berlin 2021, S. 132.
11 Vgl. *Hornung*, Datenschutzrechtliche Aspekte der Social Media. In: Hornung/Müller-Terpitz (Hrsg.), Rechtshandbuch Social Media, 2. Aufl., Berlin 2021, S. 132.

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. Mastodon ist nur eine Software von vielen, die zum Fediverse gezählt werden. Die thematische Eingrenzung auf Mastodon erfolgt insbesondere aus ökonomischen Gründen. 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 nicht zu kompliziert werden, bezieht sich dieser Aufsatz speziell auf den Betrieb einer Mastodon-Instanz. Viele dieser Ausführungen sind auch auf andere Software im Fediverse, wie Kbin, Friendica oder Calckey anwendbar. Zusätzliche rechtliche Anforderungen ergeben sich zum Beispiel für Videosharing-Plattformen wie PeerTube.[12] Andere Fragen ergeben sich auch bei den Event-Plattformen Mobilizon, gancio oder gath.io.

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-Telemedien-Datenschutz-Gesetz (TTDSG) ergeben. Die hier dargestellte Rechtslage bezieht sich auf Instanzbetreiberinnen in Deutschland, die die Instanz in Deutschland ansässigen Accountinhaberinnen zur Verfügung stellen. Probleme aus anderen Rechtsgebieten werden nur am Rande thematisiert, zum Beispiel Impressumspflichten und Haftungsfragen. Die Anforderungen, die sich aus dem neuen Gesetz für digitale Dienste, dem Digital Services Act (DSA)[13], ergeben, wären mindestens einen eigenen Aufsatz wert. Vertragsrechtliche Fragen im Nutzungsverhältnis werden hier nur soweit berührt wie dies für die Klärung der Rechtsgrundlage für die Datenverarbeitung erforderlich ist.

12 Siehe dazu Sieber, K&R 2022, 50 (53 f.) – Open-Access-Version: https://cloud.weizenbaum-institut.de/s/kEyydT72PSSpjSo.

13 Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG.

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 Accountinhaberinnen herauszugeben, ohne dass die auskunft(s)verlangende Behörde für ihre Anfrage eine Rechtsgrundlage angibt. Aufgrund der hohen Risiken für die Interessen 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 wird auch die Perspektive von (App-)Entwicklerinnen oder Accountinhaberinnen, wie beispielsweise die Frage, ob Accountinhaberinnen selbst Anbieterinnen von Telemedien sind.

2. Technische Grundlagen von Mastodon

2.1 Historische Vorbilder

Die Idee dezentraler, verteilter oder „föderaler“ sozialer Netzwerke[14] 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.[15]

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.[16] Laconica verwendete zunächst das OpenMicroBlogging-Protokoll, das später vom OStatus-Standard abgelöst wurde.[17] Der OStatus-Standard beschreibt das Zusammenspiel mehrerer verbreiteter offener Protokolle, die föderiertes MicroBlogging ermöglichen.[18] Eine

---

14 Vgl. https://de.wikipedia.org/wiki/Verteiltes_soziales_Netzwerk.
15 Siehe https://de.wikipedia.org/w/index.php?title=Extensible_Messaging_and_Presence_Protocol&oldid=234321536.
16 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.
17 Vgl. https://de.wikipedia.org/w/index.php?title=OStatus&oldid=222774690.
18 Siehe https://en.wikipedia.org/w/index.php?title=OStatus&oldid=1163781683.

wichtige Grundlage dafür bilden insbesondere Atom- und RSS-Feeds,[19] und schließlich ActivityStreams[20]. Später steigt identi.ca auf die effizientere pump.io-Software um, deren Protokolle auch als Vorbild für ActivityPub dienen.[21] Weitere frühe Projekte sind diaspora und Mistpark bzw. Friendica. Die Einigung auf ActivityPub hat schließlich sehr zur Interoperabilität zwischen diesen Diensten beigetragen. Ein wichtiger Faktor ist aber auch, dass diese Projekte meist Copyleft-Lizenzen wie die Affero GNU General Public License (AGPL)[22] 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.[23] Andere Projekte verfolgen einen Peer2Peer-Ansatz, wie Twister und Secure Scuttlebutt.[24] Diese Ansätze sind interessant und möglicherweise datenschutzfreundlicher, scheinen sich gegenüber ActivityPub aber bis auf Weiteres nicht durchzusetzen.[25]

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.[26]

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.[27] ActivityPub baut wie

19 Siehe https://www.w3.org/community/ostatus/wiki/The_Basics.
20 https://www.w3.org/TR/activitystreams-core/.
21 Siehe https://en.wikipedia.org/w/index.php?title=Pump.io&oldid=1125130270.
22 https://www.gnu.org/licenses/agpl-3.0.html.
23 Vgl. https://en.wikipedia.org/w/index.php?title=Comparison_of_software_and_protocols_for_distributed_social_networking&oldid=1163579354.
24 Vgl. https://en.wikipedia.org/w/index.php?title=Comparison_of_software_and_protocols_for_distributed_social_networking&oldid=1163579354.
25 Vgl. https://ariadne.space/2019/01/07/activitypub-the-worse-is-better-approach-to-federated-social-networking/.
26 https://web0.small-web.org/.
27 Siehe https://de.wikipedia.org/w/index.php?title=ActivityPub&oldid=235047239.

schon OStatus auf der ActivityStreams-Spezifikation auf, die wie ActivityPub von der Social Web Working Group des W3C erarbeitet wurde.[28] Mit ActivityStreams wird eine Syntax für „Activities“ in sozialen Medien beschrieben, unter Verwendung des JSON-Dateiformats.[29] Die verwendeten Begriffe wie *Activity*, *Object*, *Actor* oder *Collection* werden im Activity Vocabulary definiert.[30]

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.[31] Allerdings spielt das Client-to-Server-Protokoll nur eine untergeordnete Rolle, da es insbesondere durch die sogenannte MastoAPI „überlagert“ wird.[32]

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.

Sendet eine Accountinhaberin A beispielsweise einen direkten Beitrag an Accountinhaber B, „postet“ sie diese zunächst in ihre eigene Outbox. Der Server A verpackt die Nachricht in eine *Create Activity* und sendet diese an die Inbox der B. Die B kann anschließend die Nachricht von ihrer Inbox abrufen. Diesem Prinzip nach würde ein öffentlich geposteter Beitrag von der Outbox der A an die Inboxes aller Actor gesendet werden, die der A 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.

---

28 Siehe https://www.w3.org/TR/activitypub/; https://www.w3.org/TR/activitystreams-core/.
29 Siehe https://www.w3.org/TR/activitystreams-core/.
30 Siehe https://www.w3.org/TR/activitystreams-vocabulary/.
31 Siehe https://www.w3.org/TR/activitypub/.
32 Vgl. https://flak.tedunangst.com/post/ActivityPub-as-it-has-been-understood.

2.2.2 „MastoAPI"

Mastodon weicht nicht nur wesentlich vom Client-to-Server-Protokoll von ActivityPub ab,[33] sondern ergänzt die W3C-Empfehlung insgesamt in einiger Hinsicht.[34] 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 sog. Mastodon API (auch „MastoAPI" genannt) orientieren.[35]

Der ActivityPub-Standard schlägt insbesondere noch keinen bestimmten Mechanismus für die Authentifizierung und Autorisierung vor.[36] Mastodon verwendet HTTP-Signaturen, um zu verifizieren, dass eine Activity tatsächlich von einem bestimmten Actor stammt.[37] Auf Client-to-Server-Ebene kommt auch der OAuth-Standard zum Einsatz, um den Client gegenüber dem Server zu autorisieren.[38]

Mastodon verwendet außerdem WebFinger, das nicht Teil von ActivityPub ist, aber auch vom OStatus-Standard erfasst wird.[39] WebFinger wird in diesem Fall dazu verwendet, anhand eines 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.[40] 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.[41]

---

33 Siehe https://activitypub.rocks/implementation-report/.
34 Vgl. https://blog.soykaf.com/post/activity-pub-in-pleroma/, zitiert nach https://flak.tedunangst.com/post/ActivityPub-as-it-has-been-understood.
35 Vgl. https://blog.soykaf.com/post/activity-pub-in-pleroma/, zitiert nach https://flak.tedunangst.com/post/ActivityPub-as-it-has-been-understood.
36 Siehe https://www.w3.org/TR/activitypub/#authorization.
37 Siehe https://docs.joinmastodon.org/spec/security/.
38 Siehe https://docs.joinmastodon.org/methods/oauth/.
39 Siehe https://docs.joinmastodon.org/spec/webfinger/; Vgl. https://en.wikipedia.org/w/index.php?title=OStatus&oldid=1163781683.
40 Danke an *@tobias@social.diekershoff.de* für diesen Hinweis.
41 Siehe https://docs.joinmastodon.org/user/moderating/.

2.3 Föderation und Deföderation bei Mastodon

Eine Mastodon-Instanz empfängt alle Beiträge von Accountinhaberinnen, denen eine Accountinhaberin der eigenen Instanz folgt. Umgekehrt übermittelt sie die Beiträge der Accountinhaberinnen an alle Instanzen, auf denen sich eine Followerin dieser Accountinhaberin befindet. Darüber hinaus können auch sog. Relays eingebunden werden, mit denen Instanzen „unbekannten" Instanzen oder Hashtags folgen können.[42]

Anders funktioniert die Föderation, wenn der *Limited Federation Mode* aktiviert ist, der allerdings den *Secure Mode* (auch *Authorized Fetch*) voraussetzt.[43] 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.[44] Die weichere Variante stellt das „Stummschalten" dar, bei dem die Inhalte der stummgeschalteten Instanzen nicht mehr in der föderierten Timeline auftauchen.[45] 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.[46] Allerdings verwendet Mastodon als Default-Einstellung (noch) Linked Data-Signaturen.[47] 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.[48] Wenn sich die geblockte Accountinhaberin 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.[49]

---

42 Siehe zum Beispiel https://relay.fedimins.net/.
43 Siehe https://docs.joinmastodon.org/admin/config/ und https://docs.joinmastodon.org/spec/activitypub/#secure-mode.
44 Vgl. https://docs.joinmastodon.org/spec/activitypub/#Block und https://www.w3.org/TR/activitypub/#block-activity-outbox.
45 Vgl. https://docs.joinmastodon.org/methods/accounts/#mute.
46 Vgl. https://docs.joinmastodon.org/methods/admin/domain_blocks/.
47 Siehe https://docs.joinmastodon.org/spec/security/#ld.
48 Siehe https://docs.joinmastodon.org/spec/security/#http.
49 Vgl. https://docs.joinmastodon.org/admin/config/#disallow_unauthenticated_api_access; danke an @Curator@mastodon.art für den Hinweis.

2.4 Datenverarbeitungen mit Mastodon

Die wesentliche Funktion von Mastodon besteht darin, sich mit anderen Fediverse-Accounts zu verbinden, mit diesen Inhalte zu teilen und zu interagieren. Im Folgenden wird genauer beschrieben, welche (personenbezogenen) Daten bei den hier wichtigsten Aktivitäten auf einer Mastodon-Instanz verarbeitet werden.

2.4.1 Besuch der Webseite einer Mastodon-Instanz

Bereits bei dem Besuch einer Mastodon-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.

Bei dem Aufruf der Webseite werden zwingend bestimmte Daten auf dem Server verarbeitet, damit die Webseite der Besucherin überhaupt angezeigt werden kann.[50] 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.[51]

Davon unabhängig ist die Servereinstellung, wie lange der Server derartige Log-Dateien speichert.[52]

Eine Verbindung der Accountinhaberin 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.

---

50 Vgl. https://developer.mozilla.org/en-US/docs/Web/HTTP.
51 https://de.wikipedia.org/w/index.php?title=User_Agent&oldid=214516660.
52 Vgl. BGH, Urteil vom 16. Mai 2017 – VI ZR 135/13 –, BGHZ 215, 55-69.

Beim Besuch einer Mastodon-Instanz wird außerdem ein Cookie namens _mastodon_session über den Webbrowser im Speicher der Besucherinnen abgelegt.[53] Es handelt sich hierbei um ein „Rails Session Cookie“, das zusammen mit dem Cookie _session_id dazu dient, den Status des Login-Prozesses zu speichern (z. B. bei einer Zwei-Faktor-Authentifizierung).[54] Zudem leitet das Cookie die Accountinhaberin nach dem Login auf die letzte besuchte Seite und speichert zusammen mit dem Cookie _session_id die Session der Accountinhaberin.[55]

Eine Besonderheit bei Mastodon stellt das Einbinden von Medien, insbesondere von Videos, dar. Wenn Accountinhaberinnen Links auf Video-Hostingdienste wie YouTube oder auch auf PeerTube-Instanzen teilen, werden diese im Beitrag in einem sog. iFrame eingebettet.[56] Auch Accountinhaberinnen, 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.[57] 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 Accountname, ein Passwort und gegebenenfalls ein Grund für den

53 Auf den Instanzen der Mastodon gGmbH mastodon.social und mastodon.online scheint dieses Cookie nicht mehr eingesetzt zu werden.
54 Siehe https://github.com/mastodon/mastodon/issues/1181.
55 Siehe https://github.com/mastodon/mastodon/issues/23843,
56 Siehe https://docs.joinmastodon.org/entities/PreviewCard/#video
57 Vgl. nur https://github.com/mastodon/mastodon/issues/877; https://github.com/mastodon/mastodon/issues/7601.

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.

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.[58]

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 Gefolgten ist öffentlich zugänglich. Auch die Indexierung durch Suchmaschinen wird zunächst erlaubt. „Per default“ werden auch Folgeanfragen automatisch bestätigt.

2.4.4 Login-Prozess

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

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.

---

58 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 Accountinhaberinnen richtet sich im Wesentlichen nach der W3C-Empfehlung.[59] Sendet eine Accountinhaberin 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 Accountinhaberin 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 Accountinhaberin einen neuen Beitrag, wird dieser in der Datenbank des Servers gespeichert und als *Create Activity* zumindest an alle Instanzen gesendet, auf denen jemand dieser Accountinhaberin folgt. Wie dieser Beitrag veröffentlicht wird und an welche Instanzen der Beitrag übermittelt wird, hängt davon ab, welche Sichtbarkeit die Accountinhaberin für diesen Beitrag eingestellt hat. Nach der Veröffentlichung kann diese Einstellung nicht geändert werden.

Das Sichtbarkeitskonzept von Mastodon unterscheidet sich etwas vom ActivityPub-Standard. Auch bei Mastodon können Beiträge öffentlich zugänglich gemacht werden. 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.[60] Öffentliche Beiträge werden vom Server an die Sammlung as:*public* adressiert und somit an alle Instanzen übermittelt, auf denen mindestens ein Account der Accountinhaberin folgt.[61] 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. Diese Beiträge werden nur Followerinnen zugänglich gemacht.[62] Direkte Beiträge werden nur an die Instanzen von Accounts übermittelt, die im Beitrag erwähnt werden, und sind nur für diese Accounts

59 Vgl. https://docs.joinmastodon.org/spec/activitypub/#supported-activities-for-profiles; https://blog.joinmastodon.org/2018/07/how-to-make-friends-and-verify-requests/.
60 Vgl. https://docs.joinmastodon.org/admin/config/#disallow_unauthenticated_api_access; danke an @Curator@mastodon.art für den Hinweis.
61 Siehe https://docs.joinmastodon.org/spec/activitypub/#Mention.
62 Siehe https://docs.joinmastodon.org/spec/activitypub/#Mention.

zugänglich.[63] 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.[64]

Eine Ende-zu-Ende-Verschlüsselung der direkten Beiträge ist vom ActivityPub-Standard nicht vorgesehen und auch von Mastodon (noch) nicht umgesetzt.[65] Das bedeutet, dass Instanzbetreiberinnen Zugriff auf alle Inhalts- und Metadaten der Accounts auf der Instanz haben. Sie haben auch Zugriff auf Antworten auf Umfragen, die von Accountinhaberinnen erstellt wurden. Diese Information wird benötigt, damit Accountinhaberinnen nicht mehrmals abstimmen können.[66]

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.[67] 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.[68]

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.[69] Diese Informationen sind auf der Webseite des Originalbeitrags öffentlich einsehbar. Wird lediglich eine Kopie auf einem

63 Siehe https://docs.joinmastodon.org/spec/activitypub/#Mention.
64 Siehe https://docs.joinmastodon.org/spec/activitypub/#Mention.
65 Vgl. https://github.com/mastodon/mastodon/pull/13820.
66 Vgl. https://docs.joinmastodon.org/entities/Poll/#voted.
67 Vgl. https://docs.joinmastodon.org/spec/activitypub/#status.
68 Vgl. nur https://github.com/Automattic/wordpress-activitypub/issues/16.
69 Siehe https://docs.joinmastodon.org/spec/activitypub/#status.

föderierenden Server abgerufen, wird dort nur ein Teil dieser „Likes“ oder „Boosts“ angezeigt. Mittels „Boosten“ eines Beitrags wird der Beitrag auch an alle Accountinhaberinnen übermittelt, die dem boostenden Account folgen. Auf diese Weise wird der Empfängerkreis öffentlicher Beiträge erweitert.

2.4.5.5 Blocken und stummschalten

Auch Accountinhaberinnen können andere Instanzen oder Accounts „stummschalten“ oder „blocken“.[70] Schaltet eine Accountinhaberin einen anderen Account stumm, werden nur für die Stummschaltende die Beiträge des stummgeschalteten Accounts nicht mehr angezeigt.[71] 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.

70 Vgl. https://docs.joinmastodon.org/spec/activitypub/#Block und https://www.w3.org/TR/activitypub/#block-activity-outbox.

71 Siehe https://docs.joinmastodon.org/user/moderating/#mute.

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.[72] Auch staatliche Institutionen, die eine Mastodon-Instanz betreiben, sind direkt an Grundrechte gebunden.[73] Das betrifft zum Beispiel die Instanz „social.bund.de“, die aktuell noch vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) betrieben wird, sowie die vom Europäischen Datenschutzbeauftragten betriebene Instanz „EU Voice“. 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. Europäische Institutionen sind an die Grundrechte-Charta der EU gebunden, insbesondere an das Recht auf Schutz personenbezogener Daten aus Art. 8 GrCh und an das Recht auf Achtung des Privat- und Familienlebens aus Art. 7 GrCh. 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 Accountinhaberinnen anderer Instanzen gespeichert. Wenn beispielsweise eine Social-Media-Beauftragte einer staatlichen Institution Beiträge von Accountinhaberinnen 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.[74] Der Betrieb einer eigenen Mastodon-Instanz ist als relativ milder Eingriff anzusehen. Einer genaueren Prüfung bedarf es hingegen, wenn sich Behörden auf Mastodon-Instanzen von Privatpersonen oder Unternehmen registrieren. Staatliche Accountinhaberinnen sollten sich in diesem Fall zumindest ausreichende Einflussmöglichkeiten auf Instanzbetreiberinnen vorbehalten, etwa im Wege eines

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

Auftragsverarbeitungsvertrags. Für private Instanzbetreiberinnen bedeutet dies zusätzlichen 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 nur indirekt aus, das heißt im Bereich des Datenschutzes vor allem bei der Auslegung der DSGVO durch die Gerichte.[75] Da insoweit EU-Recht angewendet wird, wird das deutsche Grundgesetz von der Grundrechte-Charta der EU überlagert.[76]

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.[77] Der Staat soll aber auch Anreize für die Verbreitung datenschutzfreundlicher Technologien schaffen. Aus rechtspolitischer Sicht ist der Staat daher gefordert, Alternativen wie das Fediverse datenschutzrechtlich zu privilegieren.

Ergänzend zur DSGVO können auch zivilrechtliche Ansprüche auf Schadensersatz nach § 823 BGB oder auf Unterlassung nach § 1004 BGB analog in Betracht kommen. Das allgemeine Persönlichkeitsrecht ist schließlich als „sonstiges Recht“ vom Schutz dieser Vorschriften erfasst. Dazu gehört zum Beispiel das Recht, nicht mit Werbe-E-Mails belästigt zu werden.[78]

---

75 Vgl. BVerfG, Beschl. v. 11.04.2018 – 1 BvR 3080/09, NJW 2018, 1667 (1668).
76 *Hornung*, Datenschutzrechtliche Aspekte der Social Media. In: Hornung/Müller-Terpitz (Hrsg.), Rechtshandbuch Social Media, 2. Aufl., Berlin 2021, S. 133.
77 *Hornung*, Datenschutzrechtliche Aspekte der Social Media. In: Hornung/Müller-Terpitz (Hrsg.), Rechtshandbuch Social Media, 2. Aufl., Berlin 2021, S. 137 f.
78 Vgl. BGH, Urteil vom 15.12.2015 – VI ZR 134/15.

4. Rechtliche Einordnung des Fediverse

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. Fraglich ist zum Beispiel, ob eine Mastodon-Instanz oder das Fediverse ein soziales Netzwerk im rechtlichen Sinne ist. Damit ist die Frage verbunden, ob es sich bei Mastodon-Instanzen um Plattformen zur Individualkommunikation handelt. Diese Abgrenzung ist indirekt auch für das Datenschutzrecht wichtig, da für diese verschiedenen Dienste jeweils andere Vorschriften des TTDSG gelten. Es könnten außerdem bereits Zweifel daran aufkommen, dass Instanzbetreiberinnen überhaupt einen „Dienst der Informationsgesellschaft" anbieten.

4.1 Dienst der Informationsgesellschaft

Eine grundlegende Frage ist, ob Betreiberinnen von Fediverse-Instanzen „Diensteanbieter" sind. Der Begriff geht zurück auf die Richtlinie über den elektronischen Geschäftsverkehr[79] und wird auch vom neuen DSA aufgegriffen.[80] „Dienste der Informationsgesellschaft" werden definiert als „jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung".[81]

Auf das Fediverse oder auf Mastodon-Instanzen scheint der Begriff des „Dienstes" nicht zu passen. Schließlich bieten die allermeisten Instanzbetreiberinnen eine kostenlose Registrierung an. Es sind bisher auch keine Instanzen bekannt, die sich über Werbung finanzieren oder die von den Accountinhaberinnen bereitgestellte Daten verwerten. Der Begriff der „Dienstleistung" scheint auch vorauszusetzen, dass zwischen Instanzbetreiberinnen und Accountinhaberinnen ein Vertrag geschlossen wird. Viele Mastodon-Instanzen werden aber mehr oder weniger ehrenamtlich betrieben, womit fraglich ist, ob ein solches Angebot als Dienstleistung bezeichnet werden kann. Die Formulierung „in der Regel gegen Entgelt" wirft die Frage auf, ob die Mastodon-Instanz mit anderen Mastodon- oder Fediverse-Instanzen zu vergleichen ist[82] oder

79 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.

80 Art. 3 a) und g) DSA.

81 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.

82 So *John/Müller/Rennert*, GRUR 2023, 691 (697).

vielmehr mit „klassischen“ sozialen Netzwerken wie Twitter.[83] *John/Müller/Rennert* sprechen sich für einen Vergleich mit anderen Mastodon-Instanzen aus, die in der Regel unentgeltlich seien.[84] Damit wird aber möglicherweise die Anwendbarkeit des DSA vorschnell abgelehnt. Ihrem Argument, dass unentgeltliche Dienste privilegiert werden sollen, ist an sich zuzustimmen.[85] Dagegen spricht, dass Mastodon aus einer objektiven Verbrauchersicht (dem „Mainstream“) einen Ersatz für Twitter darstellt. Die Ansicht der Autorinnen lässt auch unberücksichtigt, dass der Begriff des Dienstes der Informationsgesellschaft eingeführt wurde, um für diese einen sicheren Rechtsrahmen zu schaffen. *John/Müller/Rennert* nehmen zugleich an, dass es sich bei Mastodon-Instanzen um Telemedien handelt, für die das Haftungsprivileg in § 10 TMG gilt.[86] Tatsächlich wird der Begriff des Telemediums teilweise weiter verstanden als sein europäisches Äquivalent.[87] Allerdings soll mit dem Begriff des (Telemedien-)Diensteanbieters gerade der Begriff des Dienstes der Informationsgesellschaft und die damit verbundenen Haftungsprivilegien in das deutsche Recht übersetzt werden.[88] Es kann bezweifelt werden, dass sich die Unterscheidung zwischen deutschem und europäischem Diensteanbieter mit dem unmittelbar und vorrangig geltenden DSA noch aufrecht erhalten lässt.

Die Frage kann jedenfalls offen bleiben, weil schon Zweifel daran bestehen, dass Mastodon-Instanzen „in der Regel unentgeltlich“ betrieben werden. Schließlich ist der Begriff des Dienstes der Informationsgesellschaft weit zu verstehen. Gewerbliche Unternehmen, die Mastodon-Instanzen betreiben, sind grundsätzlich als Diensteanbieter anzusehen.[89] In diesem Fall liegt es nahe, dass die Mastodon-Instanz zumindest auch zur Image-Pflege betrieben wird. Aber auch beispielsweise gemeinnützige Vereine können wirtschaftlich tätig werden.[90] Der europäische Gesetzgeber setzt eine zwar wirtschaftliche Tätigkeit voraus, fordert dafür aber nicht zwingend eine Gewinnerzielungsabsicht.[91] Weder ein Vertrag noch eine monetäre Gegenleistung ist notwendig.[92] Es kommt bei der Frage der Entgeltlichkeit gerade nicht darauf an, dass die

---

83 So im Ergebnis *Sieber*, K&R 2022, 50 (53) – Open-Access-Version: https://cloud.weizenbaum-institut.de/s/kEyydT72PSSpjSo.
84 Siehe *John/Müller/Rennert*, GRUR 2023, 691 (697).
85 Vgl. *John/Müller/Rennert*, GRUR 2023, 691 (697).
86 Siehe *John/Müller/Rennert*, GRUR 2023, 691 (694).
87 Dies bejaht *Spindler* in Spindler/Schmitz, Telemediengesetz, 2. Aufl. 2018, § 1 TMG Rn. 6.
88 Siehe Begr. RegE, BT-Drs. 16/3078, S. 1, 11.
89 Vgl. *Liesching*, in: Erbs/Kohlhaas (Hrsg.), Strafrechtliche Nebengesetze, Werkstand: 245. EL Februar 2023, NetzDG § 1, Rn. 4.
90 Siehe EuGH, Urt. v. 19.6.2014, EuZW 2017, 672.
91 Siehe EuGH, Urt. v. 19.6.2014, EuZW 2017, 672.
92 Vgl. Erwägungsgrund 18 der RL 2000/32/EG.

Dienstleistung von der Person bezahlt wird, der diese zugute kommt.[93] Auch der Betrieb einer Mastodon-Instanz muss auf irgendeine Weise bezahlt oder querfinanziert werden. Insofern sind jedenfalls spendenfinanzierte Instanzen als Diensteanbieter anzusehen. Im Erwägungsgrund 18 der Richtlinie über den elektronischen Geschäftsverkehr sind auch explizit solche Dienste genannt, „die Informationen, die von einem Nutzer des Dienstes stammen, speichern", unabhängig von einem Entgelt.[94] Es ist davon auszugehen, dass zumindest die Instanzen, auf denen sich andere Personen als die Betreiberinnen registrieren können, Dienste der Informationsgesellschaft sind. Dies liegt auch nahe für „Ein-Personen-Instanzen", weil diese auch Beiträge von Accountinhaberinnen anderer Instanzen speichern.

Ab dem 17. Februar 2024 gelten damit für die meisten Mastodon-Instanzen die Bestimmungen für Anbieterinnen für Vermittlungsdienste in Artt. 11-15 DSA, aber auch die Bestimmungen für Hostingdiensteanbieterinnen in Artt. 16-18 DSA.[95] Im Wesentlichen ergeben sich dadurch keine Neuerungen gegenüber dem TMG. Es wird allerdings erforderlich sein, kleine Änderungen am Meldeverfahren vorzunehmen, um den Anforderungen des Art. 15 DSA zu entsprechen.

4.2 Angrenzung zu Plattformen für die Individualkommunikation

Die zusätzlichen Vorschriften des DSA zu Online-Plattformen und auch die des NetzDG gelten nicht für Plattformen, die für die Individualkommunikation bestimmt sind.

Schwierig ist die Abgrenzung nach dem NetzDG. Dort werden lediglich Plattformen, die zur Individualkommunikation bestimmt sind, vom Anwendungsbereich ausgenommen.[96] Diese Unterscheidung ist praktisch kaum möglich, da viele Dienste, auch Mastodon-Instanzen, sowohl Funktionen für die öffentliche Kommunikation als auch für die Individualkommunikation bereitstellen.[97]

Der DSA enthält zusätzliche Vorschriften für Online-Plattformen und beschreibt diese als Hosting-Dienste, die Informationen im Auftrag einer Nutzerin speichern und öffentlich verbreiten.[98] Gemäß Art. 3 f) DSA darf es sich dabei nicht um eine unbedeutende und reine

93 Vgl. EuGH, Urt. v. 26.4.1988 – C-352/85.
94 Siehe Erwägungsgrund 18 der 2000/31/EG.
95 Vgl. Art. 93 Abs. 2 DSA.
96 § 1 Abs. 1 S. 3 NetzDG.
97 Vgl. *Liesching*, in: Erbs/Kohlhaas (Hrsg.), Strafrechtliche Nebengesetze, Werkstand: 245. EL Februar 2023, NetzDG § 1, Rn. 10; Spindler, K&R 2017, 533 (534).
98 Art. 3 f) DSA.

Nebenfunktion eines anderen Dienstes handeln, die aus objektiven und technischen Gründen nicht ohne diesen anderen Dienst genutzt werden kann.

Bei Mastodon stellt das öffentliche Teilen oder „MicroBlogging“ bestimmungsgemäß die Hauptfunktion dar, während die direkten Beiträge nebensächlich sind und nicht getrennt von der Hauptfunktion genutzt werden können. Sie sind keine Plattformen, die zur Individualkommunikation bestimmt sind. Der DSA ist also anwendbar und theoretisch auch das NetzDG.

4.3 Soziales Netzwerk

Nach dem allgemeinen Sprachgebrauch kann eine Mastodon-Instanz als soziales Medium oder soziales Netzwerk bezeichnet werden. Mastodon-Instanzen sind für den gemeinsamen Austausch bestimmt und ermöglichen es, Beiträge zu empfehlen oder zu bewerten, sich mit anderen Accountinhaberinnen zu verbinden und dadurch soziale Beziehungen herzustellen.[99] Die Besonderheit von Mastodon und anderen Fediverse-Instanzen besteht darin, dass die Accountinhaberinnen über den Dienst einer Anbieterin hinweg mit anderen interagieren können. Daher wird oft das Fediverse in seiner Gesamtheit als das soziale Netzwerk angesehen.[100] Es handelt sich jedoch vielmehr um Verbünde von sozialen Netzwerken. Schließlich ist die Föderation selbst ein sozialer Vorgang. Es sind keineswegs alle Instanzen des Fediverse miteinander verbunden. Das soziale Netzwerk ist auch nicht „Mastodon“, da es sich hierbei lediglich um eine mögliche Software handelt, mit der eine Fediverse-Instanz betrieben werden kann.

Das soziale Netzwerk taucht als Rechtsbegrifff erstmals im Netzwerkdurchsetzungsgesetz (NetzDG) auf. In § 1 Abs. 1 NetzDG werden soziale Netzwerke definiert als „Telemediendiensteanbieter, die mit Gewinnerzielungsabsicht Plattformen im Internet betreiben, die dazu bestimmt sind, dass Nutzer beliebige Inhalte mit anderen Nutzern teilen oder der Öffentlichkeit zugänglich machen“.

Eine Gewinnerzielungsabsicht setzt jedenfalls nicht voraus, dass Accountinhaberinnen einen Geldbetrag für die Nutzung der Instanz zahlen, da Gewinne zum Beispiel auch durch

---

99 Vgl. *Hohlfeld*, Das Phänomen Social Media. In: Hornung/Müller-Terpitz (Hrsg.), Rechtshandbuch Social Media, 2. Aufl., Berlin 2021, S. 15.

100 Vgl. *John/Müller/Rennert*, GRUR 2023, 691; https://de.wikipedia.org/w/index.php?title=Fediverse&oldid=234517027.

Werbeeinahmen erzielt werden können.[101] Bisher sind allerdings keine Instanzen bekannt, die sich durch Werbeanzeigen finanzieren oder gar Gewinne erzielen. Eine Gewinnerzielungsabsicht kommt insbesondere dann in Frage, wenn eine Mastodon-Instanz von einem gewerblichen Unternehmen betrieben wird.[102] Der Betrieb einer Instanz ist schließlich auch Werbung für dieses Unternehmen. Insofern kann von einer Gewinnerzielungsabsicht ausgegangen werden, wenn ein Mastodon-Account im Rahmen eines Abonnements zur Verfügung gestellt wird. Wegen der relativ hohen Kosten für den Serverbetrieb und des Arbeitsaufwands für die Moderation erscheint es aber unwahrscheinlich, mit einer einzelnen Mastodon-Instanz Gewinne erzielen zu können. Manche Instanzen schaffen es, die Serverbetriebskosten durch Spenden zu decken. Seltener können die Betreiberinnen auch Administratorinnen oder Moderatorinnen bezahlen. In den allermeisten Fällen sind Mastodon-Instanzen keine sozialen Netzwerke im rechtlichen Sinne. Auch das Urheberrechts-Diensteanbieter-Gesetz (UrhDaG) ist mangels Gewinnerzielungsabsicht nicht anwendbar.[103]

Das NetzDG kann insofern vernachlässigt werden, als dass soziale Netzwerke mit weniger als zwei Millionen registrierten Nutzerinnen nach § 1 Abs. 2 NetzDG ohnehin von den Pflichten des NetzDG befreit sind. Gelegentlich wird die Frage aufgeworfen, ob sich diese Zwei-Millionen-Grenze auf eine einzelne Instanz oder das ganze Fediverse bezieht. Bis dato existiert keine Instanz mit mehr als zwei Millionen registrierten Nutzerinnen, während die Anzahl der Fediverse-Nutzerinnen in Deutschland darüber liegt.[104] Das Fediverse als solches ist jedoch kein „Dienst". Korrekterweise ist der Dienst bei der einzelnen Mastodon-Instanz zu verorten. Dafür spricht auch der Wortlaut des § 1 Abs. 2 NetzDG, in dem von „registrierten" Nutzerinnen die Rede ist.[105] Dafür spricht auch, dass die Pflichten aus dem NetzDG nur auf Instanzebene umgesetzt werden können. Die Bezeichnung einer Mastodon-Instanz als soziales Netzwerk erscheint nur deshalb ungewohnt, weil es in den typischen „Walled Gardens" an Interoperabilität mangelt. Für die großen Anbieterinnen von interpersonellen

101 Vgl. *Liesching*, in: Erbs/Kohlhaas (Hrsg.), Strafrechtliche Nebengesetze, Werkstand: 245. EL Februar 2023, NetzDG § 1, Rn. 4.
102 Vgl. *Liesching* ebd.
103 § 2 Abs. 1 UrhDaG
104 Nach dem Stand vom 11.07.2023 wurden im Fediverse über 12 Millionen Accounts gezählt, siehe https://fediverse.observer/stats.
105 Siehe Vgl. *Liesching*, in: Erbs/Kohlhaas (Hrsg.), Strafrechtliche Nebengesetze, Werkstand: 245. EL Februar 2023, NetzDG § 1, Rn. 14.

Kommunikationdiensten wird eine solche Interoperabilität aber bald zur rechtlichen Vorgabe.[106] Bekannt ist dieses Konzept auch schon von E-Mail-Diensten.

Auch der DSA bezieht sich auf „soziale Netzwerke“, verwendet diesen Begriff jedoch nur in den Erwägungsgründen.[107] Auf soziale Netzwerke sollen die Regelungen für Anbieterinnen von Online-Plattformen Anwendung finden.[108] Der Begriff der Online-Plattform weist große Ähnlichkeiten mit dem des sozialen Netzwerks auf, fordert hingegen keine Gewinnerzielungsabsicht.[109] Die zusätzlichen Bestimmungen für Online-Plattformen gelten aber nicht für sogenannte Kleinst- und Kleinunternehmen.[110] Damit sind solche Unternehmen gemeint, die weniger als 50 Personen beschäftigen und deren Jahresumsatz bzw. Jahresbilanz 2 Milionen Euro nicht übersteigt.[111] Erst wenn Mastodon-Instanzen mehr als 45 Millionen aktive Accountinhaberinnen haben, sind die Bestimmungen für (sehr große) Online-Plattformen zu beachten.[112]

106 Siehe Art. 7 des Gesetzes über digitale Märkte (Digital Markets Act).
107 Siehe Erwägungsgrund 1 und 13 DSA.
108 Siehe Erwägungsgrund 13 DSA.
109 Vgl. Art. 3 i) DSA.
110 Art. 19 Abs. 1 DSA.
111 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
112 Art. 33 Abs. 1 und 4 DSA.

5. Adressatinnen datenschutzrechtlicher Pflichten

Aufgrund der vielen beteiligten Personen im Fediverse stellt sich die wichtige Vorfrage, ob sich die datenschutzrechtlichen Pflichten aus der DSGVO und TTDSG überhaupt an Instanzbetreiberinnen richten oder (auch) an andere Personen. Sofern die Vorschriften des TTDSG relevant sind, richten sich diese an Anbieterinnen von Telemedien. Im Rahmen der DSGVO stellt sich demgegenüber die Frage, wer „verantwortlich" für die konkrete Datenverarbeitung ist. In der DSGVO gibt es außerdem den Begriff der gemeinsamen Verantwortlichkeit, der von der Auftragsverarbeitung abzugrenzen ist.

5.1 Anbieterinnen von Telemedien

Telemedien sind elektronische Informations- und Kommunikationsdienste, wovon insoweit Rundfunk und Telekommunikationsdienste ausgenommen sind.[113] Aufgrund der Verteilung der Gesetzgebungskompetenzen zwischen Bund und Ländern hat der deutsche Gesetzgeber auf diese Weise den Begriff des Diensteanbieters in Telemedien-, Telekommunikationsdienste und Rundfunk aufgespalten.[114] Der Begriff des Telemediums wird nach allgemeiner Meinung noch weiter verstanden als der europäische Begriff des „Dienstes der Informationsgesellschaft".[115] Damit sind zweifellos auch nicht-kommerzielle Dienste, also sogar private Webseiten, Foren und (Micro)-Blogs vom Begriff des Telemediums erfasst.[116]

Das TMG dient insbesondere der Umsetzung der E-Commerce-Richtlinie.[117] Dort enthalten sind vor allem Haftungserleichterungen für Access-, Caching- und Hostingprovider, aber auch die sogenannten Impressumspflichten.[118] Mit einem Teil des TTDSG soll die EU-Richtlinie 2002/58/EG für elektronische Kommunikation (E-Privacy-RL) umgesetzt werden.[119] Im Übrigen ist die Bedeutung der Vorschriften fraglich. Das TTDSG geht der DSGVO nur vor, sofern mit dem TTDSG Regelungen der E-Privacy-RL umgesetzt werden.[120] Im Bereich des Telemediendatenschutzes betrifft das hier nur die sogenannte „Cookie-Banner"-Regelung in §

113 § 2 TTDSG i.V.m. § 1 Abs. 1 TMG.
114 Siehe *Spindler*, in Spindler/Schmitz, Telemediengesetz, 2. Aufl. 2018, § 1 TMG Rn. 1.
115 Siehe *Spindler*, in Spindler/Schmitz, Telemediengesetz, 2. Aufl. 2018, § 1 TMG Rn. 6.
116 So *Müller-Broich*, Telemediengesetz, 1. Aufl. 2012, § 1 TMG Rn. 6.
117 Siehe *Spindler* in Spindler/Schmitz, Telemediengesetz, 2. Aufl. 2018, § 1 TMG Rn. 6.
118 §§ 5, 7 ff. TMG. Näher dazu m.w.N. *Sieber*, K&R 2022, 50 (53) – Open-Access-Version: https://cloud.weizenbaum-institut.de/s/kEyydT72PSSpjSo.
119 *Herrmann* in Assion (Hrsg.), TTDSG, § 1 TTDSG Rn. 9.
120 Art. 95 DSGVO.

25 TTDSG.[121] Die anderen Vorschriften des TTDSG 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.[122]

Ob Accountinhaberinnen ebenfalls als Telemediendiensteanbieterinnen anzusehen sind, wird an dieser Stelle ausgeklammert. Die Betreiberinnen der Instanz sind es in jedem Fall. Auch wenn sie die Instanz nur für ihren eigenen Account betreiben, stellen sie eine öffentlich zugängliche Webseite bereit.

Es stellt sich lediglich die Frage, ob Instanzbetreiberinnen der sogenannten Impressumspflicht aus § 5 TMG oder jedenfalls der eingeschränkten Impressumspflicht aus § 18 des Medienstaatsvertrags unterliegen. Zweifel bestehen insofern, als dass es sich um eine private Instanz handelt, auf der nur die Betreiberin selbst einen Account besitzt. Letztendlich unterliegt diese im Regelfall jedenfalls den Informationspflichten aus der DSGVO.

5.2 Anbieterinnen von Interpersonellen Kommunikationsdiensten

Telekommunikationsdienste sind „insoweit“ vom Begriff der Telemedien ausgenommen. Das lässt den Schluss zu, dass Dienste teilweise Telekommunikationsdienste und teilweise Telemedien sein können.[123] Mit dem Europäischen Kodex für Elektronische Kommunikation (EKEK)[124] wurde der Unterbegriff des interpersonellen Kommunikationsdienstes geschaffen. Dieser soll insbesondere Messenger-, aber auch E-Mail-Dienste erfassen.[125] Ursprünglich sollten soziale Netzwerke nicht darunter fallen.[126] Gemeint waren damit vermutlich aber eher solche Plattformen und Diskussionsforen, auf denen die Inhalte öffentlich zugänglich sind.[127] Es stellt sich die Frage, ob Instanzbetreiberinnen im Hinblick auf direkte Beiträge und „follower-only“ veröffentlichte Beiträge interpersonelle Kommunikationsdienste sind. Dann würde die DSGVO auf direkte und „follower-only“-Beiträge nur eingeschränkt Anwendung finden, weil für diese bereits das Fernmeldegeheimnis nach § 3 TTDSG gilt.[128]

---

121 Vgl. Art. 5 Abs. 3 der E-Privacy-RL.
122 Siehe *Eckhardt/Lepperhoff*, in: Schwartmann/Jaspers/Eckhardt (Hrsg.), TTDSG, 1. Aufl. 2022, § 19 Rn. 11 f.
123 Vgl. *Roßnagel*, NVwZ 2007, 743; *Bender/Kahlen*, MMR 2006, 560.
124 Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11.12.2018 über den europäischen Kodex für die elektronische Kommunikation.
125 Siehe *Piltz/Quiel*, CR 2022, 263.
126 Siehe Erwägungsgrund 17 EKEK.
127 Siehe *Assion*, in: Assion (Hrsg.), TTDSG, 1. Aufl. 2022, § 3 TTDSG Rn. 85.
128 Art. 95 DSGVO i.V.m. Art. 5 E-Privacy-RL.

Das TTDSG verweist auf den Begriff des interpersonellen Kommunikationsdienstes im Telekommunikationsgesetz (TKG).[129] Demnach kommt es darauf an, dass eine Kommunikation zwischen einer endlichen Zahl von Personen ermöglicht wird und die Empfänger jeweils bestimmt werden.[130] Hingegen handelt es sich um keinen interpersonellen Kommunikationsdienst, wenn es sich dabei um eine unbedeutende und untrennbar mit einem anderen Dienst verbundene Nebenfunktion handelt.[131]

Mastodon wird gerade nicht als „Messenger" bezeichnet, anders als die föderalen Instant Messenger, die beispielsweise XMPP oder das Matrix-Protokoll nutzen. 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. Zudem spielt es eine entscheidende Rolle, wie die Funktion „beworben" wird.[132] Die Startseite einer 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 Datenschutzhinweisen beschrieben. Auch auf der Startseite der Mastodon gGmbH ist diese Funktion nicht erwähnt.[133] Die Hauptfunktion von Mastodon besteht eindeutig darin, öffentliche Beiträge zu teilen. Die verschiedenen Funktionen und Sichtbarkeitseinstellungen sind auch untrennbar miteinander verbunden.[134] Hierbei ist weniger die Erkennbarkeit für Nutzerinnen entscheidend, sondern die technische Funktionsweise.[135] Beiträge aller Sichtbarkeitsstufen werden bei Mastodon auf die gleiche Weise versendet wie öffentliche Beiträge, nur mit einer anderen Sichtbarkeit. Sie werden zudem über die gleiche Weboberfläche abgerufen und landen in der gleichen „Timeline".

Die Definition von interpersonellen Kommunikationsdiensten trifft bei Mastodon jedoch sowohl auf direkte Beiträge als auch auf „follower-only" veröffentliche Beiträge zu.[136] In beiden Fällen ist die Zahl der Empfängerinnen limitiert. Die Empfängerinnen werden außerdem von den Accountinhaberinnen selbst bestimmt. Aus technischer Sicht sind diese verschiedenen Funktionen untrennbar miteinander verbunden, aber sie sind keinesfalls unbedeutend. Ob die

---

129 §§ 2 Abs. 1 TTDSG, § 3 Nr. 24 TKG.
130 § 3 Nr. 24 TKG.
131 Art. 2 Nr. 5 EKEK; Piltz/Quiel, CR 2022, 263 (264).
132 Siehe *Piltz/Quiel*, CR 2022, 263 (267).
133 https://joinmastodon.org/.
134 So auch *John/Müller/Rennert*, GRUR 2023, 691 (698).
135 Siehe Erwägungsgrund 17; *Piltz/Quiel*, CR 2022, 263 (267).
136 Andere Ansicht (noch) *Sieber*, K&R 2022, 50 (53, 54 f.) – Open-Access-Version: https://cloud.weizenbaum-institut.de/s/kEyydT72PSSpjSo.

Funktion unbedeutend oder untergeordnet ist, ist in erster Linie aus der objektiven Sicht der Endnutzerin zu beurteilen.[137] Diese Ausnahme ist dann einschlägig, wenn die Funktion für Accountinhaberinnen nur einen sehr begrenzten Nutzen hat und von diesen kaum genutzt werden.[138] Tatsächlich werden direkte Beiträge auch für die private Kommunikation verwendet. Auch die Möglichkeit, Beiträge „follower-only" zu veröffentlichen, wird rege genutzt. Gegen die Geltung des Fernmeldegeheimnisses für soziale Netzwerke wird eingewandt, dass es Instanzbetreiberinnen erlaubt sein sollte, diese Inhalte zu überwachen, um Accountinhaberinnen vor Spam, Mobbing oder Betrug zu beschützen.[139] Eine solche paternalistische Interpretation ist jedoch abzulehnen, weil damit das Fernmeldegeheimnis nahezu ausgehebelt werden würde. Konsequenterweise sind Instanzbetreiberinnen als interpersoneller Kommunikationsdienst anzusehen, soweit es um direkte Beiträge und „follower-only" veröffentlichte Beiträge geht. Diese Beiträge sind vom Fernmeldegeheimnis geschützt, das heißt, sie dürfen grundsätzlich nicht von Instanzbetreiberinnen eingesehen werden.

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 […]".[140] Ausschlaggebend nach der DSGVO ist also, wer im konkreten Fall „Herrin der Daten"[141] ist, das heißt, wer die Entscheidungs- oder Verfügungsgewalt über die Daten innehat.[142] 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".[143]

Die Zwecke der Verarbeitung können als das „Warum" und „Wofür" einer Datenverarbeitung beschrieben werden.[144] Diese Zwecke stehen in einem engen Zusammenhang mit der

137 Siehe Erwägungsgrund 17.
138 Siehe Erwägungsgrund 17.
139 So *Assion*, in: Assion (Hrsg.), TTDSG, 1. Aufl. 2022, § 3 TTDSG Rn. 87.
140 Art. 4 Nr. 7 DSGVO.
141 *Schaffland/Holthaus* in: Schaffland/Wiltfang, DSGVO/BDS, Art. 4 Rn. 145.
142 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 41; *Schreiber*, in: Plath, DSGVO/BDSG/TTDSG, VIII. Verantwortlicher (Nr. 7), Rn. 29.
143 § 3 Abs. 7 BDSG a.F.
144 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 123.

Rechtsgrundlage[145] und sind möglichst konkret zu betrachten.[146] Unter Mittel der Verarbeitung sind beispielsweise bestimmte Verfahren, eine bestimmte Software, eine technische Infrastruktur oder auch eine bestimmte Dienstleisterin zu verstehen.[147] Über die Mittel zu bestimmen, kann auch bedeuten, sonstige Details festzulegen, wie zum Beispiel Löschfristen, die Arten der personenbezogenen Daten[148], Zugangsrechte und Kategorien betroffener Personen.[149]

Die Verantwortlichkeit wird in der Rechtsprechung des EuGH im Interesse eines wirksamen Datenschutzes weit ausgelegt.[150] Wer verantwortlich ist, ist aus der Perspektive einer durchschnittlichen betroffenen Person zu beurteilen.[151] Es kommt darauf an, was eine betroffene Person vernünftigerweise erwarten kann.[152]

Die Verantwortlichkeit ist im Hinblick auf die konkrete Datenverarbeitung oder Vorgangsreihe zu bestimmen.[153] 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.[154]. 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.[155] Die gemeinsame

---

145 Siehe *Radtke* ebd.
146 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 124.
147 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 143.
148 Vgl. EuGH, Urteil vom 10.7.2018 – C-25/17, NJW 2019, 285 (Rn. 70) – Zeugen Jehovas.
149 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 125 f.
150 Siehe nur EuGH, Urteil vom 5.6.2018 – C-210/16, EuZW 2018, 534 (536), Rn. 28 – Wirtschaftsakademie.
151 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 112.
152 Siehe Erwägungsgrund 47 der DSGVO.
153 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.
154 Siehe *Schaffland/Holthaus*, in: Schaffland/Wiltfang, DSGVO/BDS, Art. 4 Rn. 145; *Schreiber*, in: Plath, DSGVO/BDSG/TTDSG, VIII. Verantwortlicher (Nr. 7), Rn. 28.
155 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 145.

Verantwortlichkeit ist einerseits abzugrenzen von der getrennten Verantwortlichkeit mehrerer Personen, d. h. die Verantwortlichkeit für unterschiedliche Bereiche, andererseits von der Auftragsverarbeitung.[156]

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.

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.[157] Im Falle einer Auftragsverarbeitung wird die Datenverarbeitung den Accountinhaberinnen als Auftraggeberinnen zugerechnet.

Eine Auftragsverarbeitung zwischen Instanzbetreiberinnen und Accountinhaberinnen setzt eigentlich voraus, dass die Accountinhaberinnen selbst Verantwortliche sind. Nach dem Willen des europäischen Parlaments soll die Nutzung sozialer Netzwerke im Rahmen persönlicher oder familiärer Tätigkeiten aber keine Verantwortlichkeit begründen.[158] Im Umkehrschluss liegt eine Verantwortlichkeit 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.[159] Mit ihren Inhalten sprechen Accountinhaberinnen 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 Accountinhaberinnen mit ihren Beiträgen andere zu einer Reaktion. Andererseits hat der EuGH auch betont, dass die

156 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 121.
157 Siehe *Hornung*, Datenschutzrechtliche Aspekte der Social Media. In: Hornung/Müller-Terpitz (Hrsg.), Rechtshandbuch Social Media, 2. Aufl., Berlin 2021, S. 152.
158 Siehe Erwägungsgrund 18 DSGVO.
159 Vgl. *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 52.

bloße Nutzung eines sozialen Netzwerks allein nicht unbedingt eine Verantwortlichkeit für die damit verbundenen Datenverarbeitungen begründet.[160]

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.[161] Besonders an dieser Instanz ist, dass der LfDI BaWü die Daten auf Weisung der Accountinhaberinnen verarbeitet. Im Fediverse ist es jedoch eher die Ausnahme, dass eine Instanzbetreiberin gegenüber Accountinhaberinnen weisungsgebunden ist. In aller Regel liegt also keine Auftragsverarbeitung vor.[162] 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 Accountinhaberinnen 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 Datenverarbeitung.[163] 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.

---

160 Siehe EuGH, Urteil vom 5.6.2018 – C-210/16, EuZW 2018, 534 (536), Rn. 35 – Wirtschaftsakademie.

161 Siehe https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2022/12/Nutzungsbedingungen-Mastodon_LfDI_V1_1.pdf.

162 Vgl. *Bäcker*, in: Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, 43. Edition, 01.11.2021, DS-GVO Art. 2 Rn. 23.

163 Vgl. *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 143.

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.[164] 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 Administrationszugang verfügt, also beispielsweise Einblicke in Registrierungsvorgänge und Bestandsdaten von Accountinhaberinnen erhält. Sie verfügt auch über die Möglichkeit, Beiträge der Accountinhaberinnen 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.[165] 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.[166] 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

---

164 Beispiele sind https://masto.host/ und https://weingaertner-it.de/index.php/produkt-kategorie/mastodon-hosting/.

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

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

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 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.[167] 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.[168] Indem eine Instanzbetreiberin die Software lokal installiert, macht diese sich den Vorschlag zu eigen.[169]

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.[170] Die Mastodon gGmbH wäre auch rechtlich gar nicht in Lage, mit Instanzbetreiberinnen vertragliche Vereinbarungen über den

167 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.
168 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 143.
169 Vgl. *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 143.
170 Vgl. *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 141 f.

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.[171]

5.3.6 Gemeinsame Verantwortlichkeit von föderierenden Instanzbetreiberinnen

Die Frage, ob föderierende Instanzbetreiberinnen gemeinsam verantwortlich sind, wurde bereits aufgeworfen.[172] Das hätte zur Folge, dass sämtliche Instanzbetreiberinnen eine Vereinbarung miteinander treffen müssten, in der sie festlegen, wer welchen Pflichten aus der DSGVO nachkommt.[173] 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. Accountinhaberinnen könnten ihre Rechte aus der DSGVO gegenüber allen föderierenden Instanzbetreiberinnen geltend machen.[174] Die Instanzbetreiberinnen könnten außerdem für Datenschutzverstöße anderer Instanzbetreiberinnen haften.[175] Bei der Frage, ob eine gemeinsame Verantwortlichkeit vorliegt, müssen jedoch sämtliche Umstände des Einzelfalls berücksichtigt werden.[176] 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

171 Vgl. *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 143.
172 Siehe https://feddit.de/post/466443.
173 Art. 26 Abs. 1 S. 2 DSGVO.
174 Art. 26 Abs. 3 DSGVO.
175 Art. 82 DSGVO.
176 Näher dazu *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 120.

oder das originale Accountprofil verlinkt wird. Nach dem Klick auf den Link beginnt ein neuer, klar abgegrenzter Verantwortungsbereich.

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 Accountinhaberinnen 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.[177] Darin liegt ihr Unterschied zur zivilrechtlichen Störerhaftung.[178] Bei der „Gemeinsamkeit" handelt es sich um ein offenes Tatbestandsmerkmal, das Raum für Abwägungsentscheidungen im Einzelfall lässt.[179] Die gemeinsame Verantwortlichkeit dient insbesondere dem Zweck, dass sich Personen nicht aus ihrer eigenen Verantwortlichkeit winden können[180] und die Verantwortlichkeit nach der tatsächlichen (aufgeteilten) Entscheidungsbefugnis zugewiesen wird.[181] Auch das Wissen über von anderen durchgeführte Verarbeitungen kann ein Indiz für eine gemeinsame Verantwortlichkeit darstellen.[182] 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.[183] 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

177 Vgl. *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 158.
178 Näher dazu *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 94 f., 102.
179 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 94.
180 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 61 f.
181 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 66.
182 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 113 f.
183 Vgl. Art. 5 Abs. 1 a) DSGVO.

Wissen, dass die Daten für Werbezwecke verwendet werden. In einem solchen Fall wäre die Frage der gemeinsamen Verantwortlichkeit erneut zu beurteilen.

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.[184] 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.[185] Instanzbetreiberinnen verfügen über keinerlei Möglichkeiten, die Beiträge auf anderen Instanzen zu löschen. Accountinhaberinnen 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.[186] Entscheidend ist auch, ob die Instanzbetreiberinnen nach außen (scheinbar) gemeinsam auftreten.[187] 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 Accountinhaberinnen und auch Aufsichtsbehörden ist klar, an welche Instanzbetreiberinnen sie sich jeweils wenden müssen.[188] Diese Erkennbarkeit der jeweils Verantwortlichen ist ein gewichtiges Argument gegen die Annahme einer gemeinsamen Verantwortlichkeit.[189] Außerdem müssen bei der Auslegung der DSGVO auch die Grundrechte der

184 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 66.
185 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 101.
186 Vgl. *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 384.
187 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 159.
188 Vgl. Erwägungsgrund 79 der DSGVO.
189 Vgl. *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 68, 79.

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 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 Accountinhaberinnen auf werbefinanzierte soziale Netzwerke zurückwerfen.

5.3.7 Gemeinsame Verantwortlichkeit von Instanzbetreiberinnen und Accountinhaberinnen

Auch die gemeinsame Verantwortlichkeit von Instanzbetreiberinnen und Accountinhaberinnen muss im Hinblick auf die konkrete Datenverarbeitung beurteilt werden. Sie liegt jedenfalls in den Fällen nahe, in denen Accountinhaberinnen auch unabhängig von Instanzbetreiberinnen verantwortlich sind. In Ausnahmefällen ist eine eigenständige Verantwortlichkeit von Accountinhaberinnen aber gar nicht erforderlich, um eine gemeinsame Verantwortlichkeit zu begründen.[190]

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.[191] Es muss auch nicht jeder in gleicher Weise die Kontrolle über die Verarbeitung haben.[192] Im Fall von Facebook war es ausreichend, dass den Facebook-Seitenbetreiberinnen anonyme Statistiken zur Verfügung gestellt wurden.[193] Das Urteil betraf allerdings das Webtracking mittels Cookies, mit dem die Beteiligten gemeinsame wirtschaftliche Interessen verfolgten.[194] Facebook dient die Funktion dazu, ihr System der Werbung zu verbessern.[195] Den Accountinhaberinnen ermöglicht es anhand der Statistiken Kenntnis von den Persönlichkeitsprofilen ihrer Besucherinnen zu erhalten.[196]Damit können Facebook-

190 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 160.
191 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.
192 Siehe *Radtke*, Gemeinsame Verantwortlichkeit unter der DSGVO, Nomos 2021, S. 47.
193 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.
194 Siehe EuGH, Urteil vom 5.6.2018 – C-210/16, EuZW 2018, 534 (Rn. 36) – Wirtschaftsakademie.
195 Siehe EuGH, Urteil vom 5.6.2018 – C-210/16, EuZW 2018, 534 (Rn. 59) – Wirtschaftsakademie.
196 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.[197] Auf diese Weise tragen Facebook-Seitenbetreiberinnen zur Verarbeitung der personenbezogenen Daten bestimmter Seitenbesucherinnen bei und fördern diese aktiv[198] 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.[199] 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.[200] Für den EuGH war diese sog. Parametrierung entscheidend, um über die bloße Nutzung einer vorkonfigurierten Plattform hinaus eine (Mit-)Verantwortlichkeit von Accountinhaberinnen zu begründen.[201] Die Inhaberinnen eines Mastodon-Accounts hingegen können nicht beeinflussen, welchen Zielgruppen ihre Beiträge angezeigt werden. Dies hängt in erster Linie davon ab, ob andere Accountinhaberinnen 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.[202] Auch in diesem Fall dienten die Datenverarbeitungen dazu, die Werbung der Webseitenbetreiberin in Facebook zu optimieren.[203] 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 Accountinhaberinnen die Plattform mit eigenen Inhalten befüllen und so für eigene Zwecke nutzen.[204] Nach einem solchen Verständnis könnte sich die gemeinsame Verantwortlichkeit auch auf weitere Datenverarbeitungen erstrecken. Accountinhaberinnen könnten schließlich ihre

197 Siehe OVG Schleswig, Urteil vom 25.11.2021 – 4 LB 20/23, ZD 2022, 344 (348), Rn. 144.
198 Siehe EuGH ebd.
199 Siehe EuGH, Urteil vom 5.6.2018 – C-210/16, EuZW 2018, 534 (536), Rn. 36 – Wirtschaftsakademie.
200 Vgl. EuGH, Urteil vom 5.6.2018 – C-210/16, EuZW 2018, 534 (Rn. 32) – Wirtschaftsakademie.
201 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.
202 Siehe EuGH, Urteil vom 29.7.2019 – C-40/17, NJW 2019, 2755 (Rn. 75) – Fashion ID.
203 Vgl. EuGH, Urteil vom 29.7.2019 – C-40/17, NJW 2019, 2755 (Rn. 80) – Fashion ID.
204 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.

Besucherinnen dazu animieren, sich auf der gleichen Instanz zu registrieren. Dadurch tragen sie dazu bei, dass die Instanzbetreiberinnen Bestandsdaten erhalten. Ohne die Beiträge der Accountinhaberinnen 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 Accountinhaberinnen besteht, kann in der Regel von getrennten Verantwortungsbereichen ausgegangen werden. Je nachdem wie stark Instanzbetreiberinnen und Accountinhaberinnen 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 2.3.1 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 TTDSG

Im Datenschutzrecht gibt es kein „belangloses" Datum.[205] Obwohl die beim Besuch einer Instanz verarbeiteten Daten eher technischer Natur sind, sind grundsätzlich alle personenbezogenen oder personenbeziehbaren Informationen vom Datenschutzrecht erfasst.[206] 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 TTDSG auskunftspflichtig gegenüber Ermittlungsbehörden und Geheimdiensten sein, welche ohne Weiteres einen Personenbezug herstellen können.

In Bezug auf „Cookies" wie die _mastodon_session ist § 25 TTDSG vorrangig anzuwenden.

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 Accountinhaberinnen öffentlich

---

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

macht, besteht für die Haushaltsausnahme kein Raum.[207] 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 TTDSG 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.[208]

6.2 Rechtsgrundlagen für die Datenverarbeitung

Auch die beim Besuch einer Mastodon-Instanz notwendigen Datenverarbeitungen müssen von einer Erlaubnisnorm gedeckt sein.[209]

Die Verarbeitung der IP-Adresse, der eingegebenen URL, dem Zugriffszeitpunkt und der im User-Agent mitgelieferten Daten sollte nicht auf Art. 6 Abs. 1 a) DSGVO gestützt werden. Die Einwilligung kann auch durch eine „eindeutige bestätigende Handlung" erteilt werden.[210] 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, 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 Mastodon-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.[211] Teilweise wird die Speicherung von Log-Dateien damit

---

207 Vgl. EuGH, Urteil vom 6. November 2003 – C-101/01 –, juris (Rn. 47).
208 Vgl. *Schneider*, in: Assion (Hrsg.), TTDSG, § 19 Rn. 14.
209 Art. 5 Abs. 1 a) DSGVO.
210 Siehe *Frenzel*, in: Paal/Pauly (Hrsg.), DS-GVO, 3. Aufl. 2021 DS-GVO Art. 6 Rn. 11.
211 Art. 5 Abs. 1 c) und e) DSGVO.

begründet, dass sie dazu verwendet werden können, Distributed-Denial-of-Service (DDoS)-Angriffe zu verhindern.[212] Zum Beispiel können die IP-Adressen der Angreiferinnen auf eine Sperrliste gesetzt werden.[213] Ein weiteres Argument ist die potenzielle Speicherung und Identifizierbarkeit der Angreiferinnen als Abschreckungsmaßnahme.[214] 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.

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 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 Accountinhaberinnen 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.

Die Verwendung des lokalen Speichers durch die _session_id und die _mastodon_session ist gemäß § 25 Abs. 2 Nr. 2 TTDSG erlaubt. Personen, die eine Mastodon-Instanz im Browser aufrufen, wollen ausdrücklich diese Webseite in Anspruch nehmen. Es handelt sich um integrative Bestandteile der Software Mastodon, die einen klar eingeschränkten, technischen Zweck verfolgen. Eine Einwilligung in Form eines interaktiven „Cookie-Banners“ ist daher für diese „Cookies“ nicht erforderlich.

---

212 Vgl. BGH, Urteil vom 16. Mai 2017 – VI ZR 135/13 –, BGHZ 215, 55-69.
213 Siehe https://docs.joinmastodon.org/admin/moderation/#blocking-by-ip.
214 Vgl. BGH, Urteil vom 16. Mai 2017 – VI ZR 135/13 –, BGHZ 215, 55-69.

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 Accountinhaberinnen 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 2.3.2) können als Bestandsdaten bezeichnet werden. Bei den im Rahmen eines Log-ins verarbeiteten Daten (siehe 2.3.3) handelt es sich um Nutzungsdaten, während sich die unter 2.3.5 und 2.3.6 beschriebenen Vorgänge auf Inhaltsdaten beziehen.

7.1 Anwendbarkeit von DSGVO und TTDSG

In Hinblick auf den _session_id-Cookie, der im Rahmen des Login-Prozesses im Browser der Accountinhaberinnen gespeichert wird, gilt § 25 TTDSG.

Für direkte Beiträge und „follower-only“ Beiträge sind die Regelungen für Telekommunikationsdienste nach den §§ 3 ff. TTDSG anwendbar.

Im Übrigen findet die DSGVO Anwendung. Für die Haushaltsausnahme besteht im Verhältnis zu Accountinhaberinnen kein Raum. Sobald Instanzbetreiberinnen anderen Personen Accounts zur Verfügung stellen, wird die Instanz nicht mehr rein für persönliche Zwecke genutzt. In seltenen Fällen kann sich eine Ausnahme für „Familieninstanzen“ ergeben.[215]

7.2 Rechtsgrundlagen für die Datenverarbeitung

Die Rechtsgrundlage für die Nutzung des lokalen Speichers durch die _session_id ist § 25 Abs. 2 Nr. 2 TTDSG. Dieser „Cookie“ hat den Zweck, dass Accountinhaberinnen sich beim nächsten Besuch der Webseite nicht erneut einloggen müssen. Damit, dass Accountinhaberinnen sich am Ende eines Besuchs nicht ausloggen, äußern sie den ausdrücklichen Wunsch, sich beim nächsten Besuch nicht wieder einloggen zu müssen.

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.[216] Damit soll verhindert werden, dass sich Spam-Accounts nach einer Sperrung erneut registrieren können. Der Nutzen dieser

215 Vgl. *Schäfer*, in: MüKo BGB, 8. Aufl. 2020, § 662 Rn. 27.
216 https://docs.joinmastodon.org/methods/admin/ip_blocks/.

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 Accountinhaberinnen entgegen, insbesondere deren Recht auf Datenschutz. Instanzbetreiberinnen können zwar anhand einer IP-Adresse die Accountinhaberinnen 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.[217] Im Rahmen einer Interessenabwägung überwiegt das Interesse der Accountinhaberinnen an einer anonymen Nutzung ihres Mastodon-Accounts. Es fehlt damit an einer Rechtsgrundlage für die Speicherung von IP-Adressen der Accountinhaberinnen.

Die Rechtsgrundlage für direkte Beiträge und „follower-only" veröffentlichte Beiträge richtet sich allein nach § 6 Abs. 1 TTDSG. Die übrigen Daten müssen Instanzbetreiberinnen ebenfalls verarbeiten, um Accountinhaberinnen die Nutzung ihres Accounts zu ermöglichen. Das betrifft die Speicherung der im Rahmen der Registrierung angegebenen Bestandsdaten und der Profilinformationen sowie die Veröffentlichung der von Accountinhaberinnen verfassten Beiträge und deren Übermittlung an andere Fediverse-Instanzen. Die Datenverarbeitungen sind gem. Art. 6 Abs. 1 b) DSGVO erlaubt, damit die Inhaberinnen eines Accounts diesen gemäß der Nutzungsbedingungen verwenden können.

Es ist nicht empfehlenswert, diese Datenverarbeitungen auf eine 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 Accountinhaberinnen dokumentieren und gegebenenfalls den Aufsichtsbehörden nachweisen können.[218] Allein aus der Tatsache, dass eine Registrierung ohne Setzen des Häkchens nicht möglich ist, lässt sich eine Einwilligung 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

---

217 Ein solcher Fall hat sich erst kürzlich bei einer US-amerikanischen Instanz ereignet, siehe https://kolektiva.social/@admin/110637031574056150.

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

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. 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 Accountinhaberinnen bestehen. Schließlich werden Instanzen oft ehrenamtlich oder als gegenseitige Hilfe betrieben. Die Instanzbetreiberinnen möchten sich in der Regel nicht rechtlich binden und die ständige Verfügbarkeit der Instanz gewähreisten. Für einen Rechtsbindungswillen spricht jedoch, dass Instanzbetreiberinnen von Accountinhaberinnen einfordern, die Nutzungsbedingungen und Verhaltensregeln zu beachten.[219] Accountinhaberinnen 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.[220] 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.[221] Dieser Gedanke lässt sich auch auf vertragsähnliche Vertrauensverhältnisse übertragen, wie Gefälligkeiten oder Mitgliedschaften in Vereinen.[222] Dazu zählt auch die Entscheidung, einen Account auf einer Mastodon-Instanz zu nutzen und die dafür erforderlichen Datenverarbeitungen zuzulassen. Instanzbetreiberinnen müssen bestimmte Daten verarbeiten, um Accountinhaberinnen die Nutzung ihres Accounts zu ermöglichen.

Auch die Übermittlung der Beiträge an andere Fediverse-Instanzen ist Gegenstand des zwischen Instanzbetreiberin und Accountinhaberin geschlossenen Nutzungsvertrags. Insofern

---

219 Vgl. *Kreutz*, ZUM 2018, 162 (166 f.).
220 Siehe nur EuGH Urteil vom 4. Juli 2023 – C 252/21, Rn. 93, 98 f.
221 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.
222 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.

ist diese Übermittlung auch dann zulässig, wenn eine in Drittländern betriebene Instanz mit der eigenen Instanz föderiert.[223]

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 Accountinhaberinnen geschlossen werden. Aber auch politische Meinungen zählen zu den besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO.

Sofern Accountinhaberinnen sensible Daten öffentlich teilen, ist deren Verarbeiten nach Art. 9 Abs. 2 e) DSGVO erlaubt. Ein Problem besteht aber dann, wenn Accountinhaberinnen bei Umfragen antworten, die sensible Themen betreffen. 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 Accountinhaberinnen eine Alternative zu datenschutzgefährdenden sozialen Netzwerken zu bieten. Solche Organisationen können sich zur Verarbeitung dieser Bestandsdaten, unabhängig von ihrer Rechtsform, auf die Erlaubnis in Art. 9 Abs. 2 d) DSGVO berufen, sofern sie in ihrer Ausrichtung den dort genannten Organisationen entsprechen.

Instanzen, deren Domain-Namen oder thematische Ausrichtung Rückschlüsse auf sensible Informationen zulässt, dürfen also nur ohne Gewinnerzielungsabsicht betrieben werden. In den engen Grenzen des für die Nutzung der Instanz Erforderlichen dürfen diese Instanzbetreiberinnen auch sensible Informationen verarbeiten.

7.3 Informations- und Auskunftsrechte

Die Informationspflichten gegenüber Accountinhaberinnen aus Art. 13 DSGVO stellen die meisten Instanzbetreiberinnen ebenfalls vor Herausforderungen.

223 Artt. 44, 49 Abs. 1 b) DSGVO.

Gemäß Art. 13 Abs. 1 e) DSGVO müssen Instanzbetreiberinnen gegebenenfalls über Empfängerinnen oder Kategorien von Empfängerinnen informieren. Empfängerinnen sind insbesondere Accountinhaberinnen und Betreiberinnen anderer Instanzen, die der betroffenen Accountinhaberin folgen oder einer Person folgen, die den Beitrag „geboostet“ hat. In der Administrationsoberfläche können Instanzbetreiberinnen die bekannten Instanzen einsehen. Es stellt sich die Frage, ob diese Liste eigentlich auch den Accountinhaberinnen 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.[224] Grundsätzlich können Accountinhaberinnen 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.

Sofern auch Beiträge an Instanzen in Drittländern übermittelt werden, ist dies nach Art. 13 Abs. 1 f) DSGVO ebenfalls in den Datenschutzhinweisen mitzuteilen.

Die Auskunftspflichten nach Art. 15 DSGVO haben keine darüber hinausgehende Bedeutung. Es ist davon auszugehen, dass Accountinhaberinnen wissen, dass sie sich auf der Mastodon-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 Accountinhaberinnen die sie betreffenden personenbezogenen Daten zu löschen. Die von Accountinhaberinnen veröffentlichten Beiträge oder auch Profilinformationen können ohne Weiteres selbst von den Accountinhaberinnen gelöscht werden. Damit werden diese Beiträge auch aus der Datenbank des Servers gelöscht.[225]

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 Accountinhaberin selbst.

224 Siehe *Franck*, in: Gola/Heckmann, DS-GVO – BDSG, 3. Aufl. 2022, DS-GVO Art. 13 Rn. 20.
225 https://docs.joinmastodon.org/spec/activitypub/.

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.[226] Es ist schließlich möglich, dass Löschanfragen von anderen Instanzen nicht umgesetzt werden, auch weil es zwischen verschiedener Software zu Kompatibilitätsproblemen kommen kann.

Ein Accountname kann nicht ohne Weiteres gelöscht werden. Accountinhaberinnen können ihren Account über die Benutzerüberfläche löschen, nicht jedoch den Accountnamen selbst. Rein technisch ist es möglich, einen Accountnamen aus der Datenbank zu löschen. Dagegen sprechen jedoch gewichtige Sicherheitsgründe, da es ansonsten anderen Personen möglich wäre, diese Identität zu „stehlen“. Der Accountname ist insofern weiterhin notwendig, um nachvertragliche Schutzpflichten gegenüber Accountinhaberinnen zu erfüllen. In diesem Fall ist deshalb das Recht auf Löschung gemäß Art. 17 Abs. 1 a) DSGVO eingeschränkt.

7.5 Recht auf Datenübertragbarkeit

Art. 20 DSGVO gibt Accountinhaberinnen das Recht, die von ihnen bereitgestellten personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und einem anderen Verantwortlichen zu übermitteln. Accountinhaberinnen 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 Accountinhaberinnen 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.

---

226 Siehe *Nolte/Werkmeister*, in: Gola/Heckmann, DSGVO – BDSG, 3. Aufl. 2022 Art. 17 DSGVO Rn. 41.

8. Pflichten gegenüber Accountinhaberinnen anderer Instanzen

Wie unter 2.3.5 beschrieben, werden die von Accountinhaberinnen geteilten 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 Accountinhaberinnen anderer Instanzen.

8.1 Anwendbarkeit der DSGVO

Im Verhältnis zu Accountinhaberinnen anderer Instanzen ist die DSGVO anwendbar. Für deren direkte Beiträge und „follower-only" Beiträge, die mit Accountinhaberinnen der eigenen Instanz geteilt werden, gelten die Regelungen für Telekommunikationsdienste in den §§ 3 ff. TTDSG.

8.2 Rechtsgrundlagen für die Datenverarbeitung

Die Rechtsgrundlage für die Verarbeitung von direkten Beiträgen und „follower-only" Beiträgen von Accountinhaberinnen anderer Instanzen ist in § 6 Abs. 1 TTDSG zu sehen.

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.[227] Andernfalls könnten auf der Instanz ausschließlich die Beiträge der eigenen Instanz angezeigt werden. Theoretisch ist es zwar möglich, eine Mastodon-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 Accountinhaberin 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 Accountinhaberinnen, mit den Accountinhaberinnen anderer Instanzen interagieren zu können. Andernfalls wäre es erforderlich, auf zahlreichen Instanzen zusätzliche Accounts anzulegen und somit mehreren Personen die Bestandsdaten preiszugeben. Die Föderation mit anderen Instanzen ist vielmehr ein Grund dafür, dass sich die Accountinhaberinnen für einen Mastodon-Account entschieden

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

haben. Es entspricht also den Erwartungen der Accountinhaberinnen, dass Inhalte auch von anderen Instanzen aus abrufbar sind, was technisch-notwendig eine Speicherung auf anderen Servern erfordert.

8.3 Informations- und Auskunftsrechte

Auch die Zwecke und die Rechtsgrundlage einer Speicherung dieser Inhalte von Accountinhaberinnen anderer Instanzen müssen sich in den Datenschutzhinweisen wiederfinden. Gemäß Art. 13 Abs. 1 d) bzw. Art. 14 Abs. 2 b) DSGVO ist auch das berechtigte Interesse der Instanzbetreiberin an diesen Verarbeitungen zu begründen.

Wer einen Mastodon-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.

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 Accountinhaberinnen 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 Accountinhaberin 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 Accountinhaberinnen 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 Accountinhaberinnen 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 Accountinhaberinnen 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 von DSGVO

Sofern personenbezogene Daten Dritter über eine Mastodon-Instanz veröffentlicht werden, ist die DSGVO anwendbar. Auch aus Sicht von (privaten) Accountinhaberinnen greift hier die Haushaltsausnahme nicht ein. Die von der DSGVO nicht erfassten persönlichen oder familiären Tätigkeiten sind sozusagen „öffentlichkeitsfeindlich".[228] 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.[229]

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. Auch in diesem Fall greift die Haushaltsausnahme nicht, da die E-Mail-Adresse dazu dient, die Verantwortliche zu kontaktieren.

---

228 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.

229 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 Accountinhaberinnen gerechtfertigt sein. Das Interesse der Accountinhaberinnen 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 Accountinhaberinnen 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 DSGVO handeln. Nur im Ausnahmefall sind solche Beiträge zulässig, zum Beispiel weil die Dritte eingewilligt hat oder die Informationen selbst offensichtlich öffentlich gemacht.[230]

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 Accountinhaberinnen 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.

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.

---

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

9.4 Recht auf Löschung und Widerrufsrecht

Löschanfragen können grundsätzlich auch an die jeweilige Accountinhaberin 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 Accountinhaberinnen 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 Accountinhaberin. 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.[231]

231 Art. 17 Abs. 3 DSGVO.

10. Fazit

Als Ergebnis dieser juristischen Analyse lässt sich festhalten, dass der Betrieb einer Mastodon-Instanz rechtskonform gestaltet werden kann. Dabei gibt es einige Herausforderungen, insbesondere das Formulieren von vollständigen und korrekten Datenschutzhinweisen. Im Vergleich mit klassischen sozialen Netzwerken zeigt sich, dass das Fediverse an sich datenschutzfreundlich konzipiert ist. Eine Mastodon-Instanz kann aber noch datenschutzfreundlicher konfiguriert werden.

Auch wenn diese Hürde überwunden ist, bleiben manche Ausführungen mit einem Fragezeichen versehen. Das Fediverse und vor allem der Betrieb einer Mastodon-Instanz werfen neue Rechtsfragen auf, insbesondere in Bezug auf die (gemeinsame) Verantwortlichkeit der zahlreichen am Fediverse beteiligten Personen. Nach der Ankündigung von Meta, mit Threads in das Fediverse einsteigen zu wollen, gewinnt diese Frage an besonderer Brisanz. Im Fediverse sind die Verantwortungsbereiche allerdings klar abgegrenzt. Mastodon ist so konzipiert, dass den anderen Instanzbetreiberinnen grundsätzlich nicht vertraut wird.[232]

Als Schwierigkeit kommt hinzu, dass einige der relevanten Vorschriften sehr neu sind. Der DSA tritt erst im Februar 2024 in Kraft. Auch das TTDSG und der Begriff des interpersonellen Kommunikationsdienstes sind relativ neu. Damit ist die Auslegung dieser Vorschriften noch sehr unklar. Schließlich orientiert sich das Recht und seine Auslegung eher an proprietären, werbefinanzierten sozialen Netzwerken, die den DSA und das Fernmeldegeheimnis lieber umgehen möchten. 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. Dass manche dieser hier angesprochenen Probleme bisher nicht thematisiert wurden, lässt sich nur damit erklären, dass zentralisierte und proprietäre soziale Netzwerke viel gravierendere Datenschutzverstöße begehen.

Es bleiben insofern gewisse rechtliche Risiken bestehen, die Instanzbetreiberinnen in Kauf nehmen müssen. Der individuelle Datenschutz kann mit den Betrieb einer eigenen Instanz noch gesteigert werden. Wünschenswert wäre es daher, wenn der Betrieb einer eigenen Instanz noch mehr vereinfacht wird und nicht davon abhängt, dass Accountinhaberinnen das nötige Kleingeld für einen Application Service Provider besitzen. Jedenfalls sollten Mastodon-Instanzen nicht zu

232 Siehe https://blog.joinmastodon.org/2023/07/what-to-know-about-threads/.

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

Autorin
Rebecca Sieber
für die Stiftung Datenschutz

Redaktionelle Bearbeitung
Hendrik vom Lehn

Agenturpartner
KING CONSULT | Kommunikation

Version
V 1.0, Stand Dezember 2023

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