

Mastodon – eine echte datenschutzrechtliche Alternative?

Aktuell reißt die Debatte um die neue Plattform Mastodon nicht ab. Obwohl wissenschaftliche Aufsätze im Netz spärlich zu finden sind, haben viele Behörden die Plattform in der Nutzung. Doch ist sie wirklich eine rechtssichere Option? Ein genauer Blick lohnt sich.

Die Entstehung von Mastodon geht auf das Jahr 2016 zurück. In Jena durch Eugen Rochko als Non-Profit-Gesellschaft gegründet, wechselte der Firmensitz der Mastodon gGmbH nach Berlin. Finanziert wurde das Projekt über Spenden, es hat einen nicht kommerziellen Charakter. Mittlerweile hat Mastodon seinen Firmensitz in New York, der unter der folgenden Adresse erreichbar ist (vgl. <https://joinmastodon.org/de/about>):

Mastodon Inc,
228 East 45th Street Suite 9E
New York, New York 10017



Quelle: Firmenseite Mastodon

Die Plattform wird als Mikroblogging-Dienst bzw. dezentrales Netzwerk klassifiziert. Dezentrale Netzwerke sind gekennzeichnet durch jeweils eigenständige Server bei Privatpersonen oder in Unternehmen. Sie nutzen keinen zen-

tralen Server bei einem der bekannten Social-Media Dienstleister und unterscheiden sich damit wesentlich in der Funktionsweise von Vergleichsportalen, wie z. B. Twitter, jetzt X Corp.

Funktionsweise

Laut der firmeneigenen Website lässt sich die Funktionsweise wie folgt erklären (vgl. <https://joinmastodon.org/de/servers>): Zunächst benötigte das interessierte Unternehmen einen Anbieter für den Server und muss auf diesem ein Konto erstellen. Das Unternehmen verwaltet seinen Account eigenständig inklusive aller Berechtigungskonzepte und Moderationsrechte. Infolgedessen findet die Vernetzung mit anderen Personen über deren Mastodon-Profil statt (auch genannt als verschiedene Instanzen¹). Interaktionen sind nur möglich, wenn die verschiedenen Personen im Netzwerk aktiv „folgen“. Konkreter: Es wird ein Benutzername und ein Knotenpunkt benötigt. Erst dann ist die Kommunikation und die Sichtbarkeit von Feeds gewährleistet. Eine Einordnung im Sinne des Telekommunikationsgesetzes (TKG) hat die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit in ihrer Konsultation der Stiftung Datenschutz zu Mastodon vom 18. Juli 2024 vorgenommen².

Optisch ist das Netzwerk aufgebaut in Timelines mit Beiträgen von dem jeweiligen Account. Es gibt Hashtags, es gibt Follower, Inhalte können gepostet, geliked und geteilt werden. Auch hier kristallisiert sich ein wesentlicher Unterschied zu Twitter bzw. X Corp. Die Anordnung der Beiträge erfolgt chronologisch nach Erstellungsdatum und folgt nicht einem Algorithmus. Letzteres ist ein wesentlicher Bestandteil einer Open-Source-Anwendung mit nicht kommerziellem Hintergrund³.

Sollte ein Serverwechsel vollzogen werden, kann das Mastodon-Profil flexibel und unkompliziert auf die neue Serverlandschaft verschoben werden – ohne Neuanlage oder Einschränkungen. Ebenfalls möglich ist das eigene Hosting von Serverlandschaften.

Prominente Nutzer

Die Nutzung von Mastodon erfreut sich steigender Beliebtheit. Angaben zum Nutzervolumen schwanken auf unterschiedlichen Websites von 11 bis 15 Millionen Usern.

Unter den Nutzern befinden sich datenschutzrechtliche Aufsichtsbehörden, wie Sachsen-Anhalt, Sachsen, Baden-Württemberg, Bayern, Berlin, Hessen, Niedersachsen, Rheinland-Pfalz oder sogar die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit). Informiert wird über die aktuelle Auslegung der Gesetzestexte, Workshops, aber auch Geldbußen und Gerichtsurteile. Die Stiftung Datenschutz stellt auf ihrer Mastodon-Seite die Tätigkeitsberichte der jeweiligen Aufsichten zur Verfügung oder auch fortlaufende Webinare im Bereich Datenschutz.

Laut Übersicht der Landesbeauftragten für Datenschutz zählen zu den weiteren prominenten Nutzern auch Rundfunk und Kirche. Immer mehr öffentliche Instanzen rufen sogar zur aktiven Nutzung von Mastodon auf. Mit Stand der Recherche vom 18. August 2025 existiert auch des Bundestags ein aktiver Auftritt auf Mastodon.

Datenschutzrechtliche Würdigung allgemein

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat eine gute Abhandlung unter dem Link <https://social.bund.de/privacy-policy> zusammengestellt.

Sicherheitseinstellungen sowie datenschutzrechtliche Voraussetzungen liefert darüber hinaus der Leitfaden

Mastodon der Stiftung Datenschutz mit Stand September 2024⁴. Hier ist auch eine umfangreiche rechtliche Einordnung zu finden.

Serverlandschaft

Grundsätzlich wird der Mastodon-Account auf dem eigenen Server gehostet. Dennoch gilt es an dieser Stelle hervorzuheben, dass die Serverlandschaft in Europa stehen und somit allen DSGVO-Standards entsprechen sollte. Der Server muss dem aktuellen Stand der Technik entsprechen und somit gängige Verschlüsselungsmechanismen erfüllen. Eine Zertifizierung des Anbieters nach ISO 27001 bringt dies hinreichend zum Ausdruck.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit nennt in ihren Datenschutzhinweisen T-Systems als möglichen Hostingdienstleister, es könnten aber auch andere europäische Dienstleister in Frage kommen. Zu beachten ist nur der Abschluss eines sogenannten Auftragsverarbeitungsvertrages sowie die Erfassung im Verzeichnis für Verarbeitungstätigkeiten. Im Einzelfall könnte auch die Erstellung einer Datenschutz-Folgenabschätzung (DSFA) vonnöten sein. Letzteres ist an die verwendeten Datenkategorien geknüpft und fallabhängig zu prüfen.

Datenschutzhinweise

Es bedarf vollständiger und den Gesetzesbestandteilen von Art. 13 und Art. 14 DSGVO entsprechender Datenschutzhinweise. Als empfehlenswerte Orientierung können hier die Datenschutzhinweise der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zur Hilfe genommen werden:

- ▶ <https://www.bfdi.de/> dort: Datenschutzerklärung, Hinweise und Verhaltensregeln

Mit Veröffentlichung der Datenschutzhinweisen gilt selbstredend die vollumfängliche Einhaltung der Betroffenenrechte gemäß Art. 15-22 DSGVO und somit auch die Sicherstellung dieser im Unternehmen. Der Datenschutzbeauftragte muss hierfür, wie auch bei anderen Projekten,

möglichst frühzeitig in die Planung eingebunden werden, so dass von Anfang an ein datenschutzkonformer Betrieb gewährleistet wird.

In Abhängigkeit vom Account-Inhaber ergeben sich möglicherweise unterschiedliche Rechtsgrundlagen in der Nutzung für Mastodon, die nicht übertragbar sind⁵. Die Behörden nutzen die Rechtsgrundlagen Art. 6 Abs. 1 lit. e) DSGVO⁶, für Unternehmen ist möglicherweise Art. 6 Abs. 1 lit. f) DSGVO⁷ eine Option. Letzteres gilt nur in Verbindung mit einer Interessenabwägung.

Besonderes Augenmerk ist auf das Impressum und die Nutzungsbedingungen zu legen, um rechtssicher auf Ihrer Instanz zu agieren.

Sicherheitseinstellungen für Betriebssystem und Webserver

Im Bereich der technischen Absicherung sind die TOMs auf dem aktuellen Stand der Technik unerlässlich. Dies beinhaltet bspw. Empfehlungen für regelmäßige automatische Backups und das Einspielen von Updates, Festplattenverschlüsselung, TLS-Einrichtung und -Updates. Weiterhin sollte die Speicherung oder sogar das Tracking von IP-Adressen deaktiviert werden. Zu beachten ist auch die Erstellung eines hausinternen Berechtigungskonzepts für die Administration.

Eine baulich sichere Serverumgebung spielt ebenfalls in das Sicherheitskonzept mit hinein.

Nutzerregeln

Außerdem empfiehlt es sich, wie auch bei anderen Social Media Accounts in einem Unternehmen, eine Art Spielregel für die Mitarbeiter wie auch für Externe aufzustellen, um eventuellen Unsicherheiten im Blick auf korrekten Verhaltensweisen im Unternehmen entgegenzuwirken. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat hier in ihren Datenschutzhinweisen eine gute Übersicht geliefert⁸: Ziel des Angebots ist ein lebendiger Dialog mit einem verantwortungsbewussten und respektvollen Umgang miteinander. Nicht gestattet sind daher:

- ▶ Werbung/kommerzielle Beiträge, Spam, Beleidigungen, Verleumdungen, üble Nachreden, Provokation sowie Beiträge mit vulgären, gewaltverherrlichenden, diskriminierenden, rassistischen, antisemitischen, sexistischen, hasserfüllten und/oder gesetzeswidrigen Äußerungen oder Inhalten
- ▶ Beiträge ohne sachlichen Bezug zum Thema
- ▶ Beiträge mit (bloßen) Verlinkungen ohne Bezug und eigenen inhaltlichen Beitrag zum Thema
- ▶ Beiträge mit fehlerhaften oder fehlenden Quellen- oder Urheberangaben, sofern diese im Zuge eines sachgerechten Beitrags geboten sind
- ▶ Beiträge mit schutzwürdigen personenbezogenen Daten, insbesondere solchen Dritter
- ▶ Beiträge in anderer als deutscher oder englischer Sprache

Ein Verstoß gegen die Verhaltensweisen sowie die Grundrechtecharta der EU verpflichtet den Betreiber immer zu einer Anzeige.

Urheberrechte

Die Verpflichtungen und Rechte der Urhebergesetze sind jederzeit vollumfänglich für das jeweilige Land einzuhalten. Besonderes Augenmerk gilt auch dem Zitieren von fremden Meinungen oder dritten Parteien. Meinungsfreiheit ist keine Rechtfertigung für Verbreitung von Meinungen dritter Personen ohne deren Einwilligung.

Datenschutzrechtliche Würdigung durch die Autorin

Abschließend zu dieser allgemeinen datenschutzrechtlichen Würdigung sollen Risiken und Möglichkeiten aufgezeigt werden.

Ein 100%iges datenschutzkonformes Niveau ist oftmals in der Praxis nicht erreichbar, auch wenn es von Datenschutzbeauftragten angestrebt wird.

Auch Mastodon könnte meiner Einschätzung nach ein geringes Restrisiko beinhalten: So können keine Identifikationskontrollen der Nutzer durchgeführt werden. Das bedeutet im Umkehrschluss, dass das anbietende Unternehmen immer die Überwachung und Kontrolle

seiner Server inklusive aller Inhalte auf der Instanz durchführen muss. Ein Mehraufwand, der oftmals in der Praxis nicht geleistet werden kann.

Denkt man diesen Gedankengang weiter, könnte man die Annahme eines rechtsfreien Raumes zugrunde legen. Ein Fakt, der in der heutigen Zeit immer Gefahren birgt. Mastodon hat keine Kontrolle darüber, was auf den fremden Servern passiert, noch können wir uns sicher sein, dass es zu keinem ungewollten Datenabfluss in die Staaten kommt. Drittlandtransfer in die USA ist immer ein hybrides Thema, immerhin hat das Unternehmen seinen Sitz in Amerika. Umso wichtiger sind hier die Sicherheitsstandards der eigenen Server.

Im Gegenzug bietet Mastodon auch eine Vielzahl von Möglichkeiten im Vergleich zu herkömmlichen Social-Media-Plattformen. Die Server sind im Eigenbetrieb in Europa, entsprechend hat das Unternehmen die Chance, vollumfänglich die Datenschutzbestimmungen selber zu regulieren und die technischen Absicherungen eigens zu gestalten. Natürlich abgesehen vom datenschutzrechtlichen Aspekt kann das Unternehmen auch kreativ werden und die individuelle Gestaltung der Instanzen in Hinblick auf Design sowie Inhalt zu 100 % eigenverantwortlich übernehmen und kontrollieren. Der durch öffentliche Stellen ausdrücklich favorisierte Betrieb bietet uns Datenschützern eine gute Richtlinie zur sicheren Nutzung von sozialen Netzwerken.

Fazit

Mastodon stellt eine echte datenschutzfreundliche Alternative zu den zentralen sozialen Netzwerken dar. Dennoch steht die Frage des internationalen Unternehmensstandorts im Raum, der ein gewisses Restrisiko birgt. Mit den richtigen Privacy-by-design-Einstellungen gemäß Art. 25 DSGVO in Kombination mit der Einhaltung der Pflichten aus Art 32 DSGVO kann dieses aber auf ein Minimum reduziert werden⁹.

Genauere Betrachtungsweise erfordert mitunter das Verhältnis zwischen Instanzbetreiber und Account-Inhaber, da hier Vertragsverhältnisse im Sinne von Art. 26 und Art. 28 DSGVO zugrunde liegen könnten¹⁰. Zusammenfassend handelt es sich um eine echte Alternative mit minimalsten Risiken im Vergleich zu den gängigen Social-Media-Plattformen unter der Prämisse, dass die hausinternen Kapazitäten für die Verwaltung zur Verfügung gestellt werden können. ■



Desirée Petzold

Beauftragte Datenschutz

E-Mail: desiree.petzold@dz-cp.de

¹ <https://www.tagesschau.de/wirtschaft/mastodon-twitter-alternative-kurznachrichtendienst-101.html>

² https://stiftungdatenschutz.org/fileadmin/Redaktion/Dokumente/Mastodon-Leitfaden/Schreiben_BfDI_zu_Konsultation_MastodonLF.pdf

³ LfD Sachsen-Anhalt (@lfd_1sa@social.sachsen-anhalt.de) - social.sachsen-anhalt.de

⁴ https://stiftungdatenschutz.org/fileadmin/Redaktion/Dokumente/Mastodon-Leitfaden/Mastodon-Leitfaden_Web-v1_1.pdf

⁵ <https://stiftungdatenschutz.org/praxisthemen/datenschutz-bei-mastodon>

⁶ Art. 6 Abs. 1 lit. e DSGVO besagt, dass die Verarbeitung rechtmäßig ist, wenn sie zur Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

⁷ Art. 6 Abs. 1 lit. f DSGVO besagt, dass die Verarbeitung rechtmäßig ist, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

⁸ <https://www.bfdi.bund.de/DE/Meta/Mastodon/Datenschutz>

⁹ <https://stiftungdatenschutz.org/praxisthemen/datenschutz-bei-mastodon>

¹⁰ https://stiftungdatenschutz.org/fileadmin/Redaktion/Dokumente/Mastodon-Leitfaden/Schreiben_BfDI_zu_Konsultation_MastodonLF.pdf