STIFTUNG DATENSCHUTZ

# Datenschutz bei Mastodon

## Leitfaden für den Instanz-Betrieb im dezentralen Netzwerk

**Autorinnen**
Jens Kubieziel
Malte Engeler
Rebecca Sieber

**Idee und Projektleitung**
Hendrik vom Lehn

Version: 1.1

# Warum gibt es diesen Leitfaden?

Das Fediverse, ein Zusammenschluss unabhängiger sozialer Netzwerke, gilt als datenschutzfreundliche Alternative zu den zentralisierten sozialen Netzwerken wie Facebook, Instagram oder X (Twitter). Diese betreiben Profiling für Werbezwecke als Teil ihres Geschäftsmodells, obwohl die Rechtsgrundlagen dafür immer wieder Gegenstand gerichtlicher und aufsichtsbehördlicher Klärung sind. Ein weiteres Problem ist, dass internationale Datentransfers stattfinden, selbst wenn miteinander kommunizierende Personen sich innerhalb des Europäischen Wirtschaftsraums befinden. Nicht zuletzt mangelt es trotz langer Datenschutzhinweise an Transparenz.

Im Gegensatz dazu setzt das Fediverse auf ein anderes Betriebsmodell ohne Profiling. Insbesondere Microblogging-Plattformen auf Basis von Mastodon[1] finden eine große Verbreitung. Die Nutzung von Mastodon wird sogar durch einige Datenschutz aufsichtsbehörden gefördert, indem diese öffentliche Stellen aktiv zur Nutzung aufrufen und eigene Instanzen betreiben. Aber auch beim Betrieb von Mastodon gilt: Auf die richtigen Einstellungen kommt es an. Dabei hilft dieser Leitfaden.

Ein datenschutzkonformer Betrieb der Plattform ist nach Ansicht der Autorinnen[2] möglich, auch wenn in einigen Punkten rechtliche Unklarheiten bestehen, die sich nicht ohne weiteres auflösen lassen. Es braucht jedoch einen passenden Rahmen. Dies betrifft zum Beispiel rechtliche Pflichtangaben, technische Konfigurationen und die begleitende Organisation des Datenschutzes.

Dieser Leitfaden richtet sich an die Betreiberinnen von Instanzen – im Speziellen an Personen, die privat oder für eine Organisation Instanzen betreiben[3]. Dies ist jedoch nur eine allgemeine Anleitung, die nicht auf alle denkbaren Konstellationen eingeht. Für eine tiefer gehende Betrachtung des Betriebs von Fediverse-Instanzen ist begleitend zum Leitfaden ein wissenschaftlicher Aufsatz erschienen.

Die Stiftung Datenschutz möchte mit der Herausgabe dieses Leitfadens zur datenschutzkonformen Nutzung sozialer Netzwerke beitragen[4].

In die vorliegende Version 1.1 des Leitfadens sind Anmerkungen aus unserer Community eingeflossen. Auch der BfDI hat zum Leitfaden Stellung genommen. Wir bedanken uns bei allen, die sich an unserer Konsultationsphase beteiligt haben.

1 Mastodon ist die Bezeichnung einer Software, mit der Microblogging-Plattformen als Teil des Fediverse betrieben werden können. Mastodon steht als freie Software unter der AGPL zur Verfügung und kann kostenfrei eingesetzt werden. Zugleich ist Mastodon eine eingetragene Marke der Mastodon gGmbH, welche die Software entwickelt und die Website joinmastodon.org sowie die Instanzen mastodon.social und mastodon.online betreibt. Sofern nichts anderes angegeben ist, bezieht sich die Nennung von „Mastodon“ in diesem Leitfaden auf den Betrieb von Instanzen mithilfe der frei verfügbaren Mastodon-Software.

2 Für eine bessere Lesbarkeit wird in diesem Leitfaden das generische Femininum verwendet. Gemeint sind alle Menschen, aber ggf. auch juristische Personen, andere Institutionen oder Organisationen.

3 Für öffentliche Stellen, die Instanzen betreiben, gelten einige Sonderbedingungen, die nicht Gegenstand des Leitfadens sind. Auch die Inhaberinnen einzelner Accounts werden hier nicht adressiert.

4 Einzelfallberatungen oder Rechtsdienstleistungen erbringt die Bundesstiftung nicht; eine rechtliche Prüfung konkreter Fälle kann nicht geleistet werden.

# Änderungen im Vergleich zur vorherigen Version

Die erste Version dieses Leitfadens erschien im Dezember 2023. In der vorliegenden Version 1.1 aus dem September 2024 wurden folgende Änderungen vorgenommen[1]:

| Änderung | Positionen im Leitfaden | Erläuterung |
|---|---|---|
| Nationale Gesetzesänderungen berücksichtigt | Zusammenfassung des begleitend erscheinenden wissenschaftlichen Aufsatzes, Praktische Umsetzung und notwendige Musterdokumente | Vorherige Verweise auf das TMG und TTDSG durch DDG und TDDDG ersetzt. |
| Zusammenfassung des Aufsatzes mit Änderungen im Aufsatz auf einen Stand gebracht. | Zusammenfassung des begleitend erscheinenden wissenschaftlichen Aufsatzes | Einordnung als digitaler Dienst und Bezüge zum DSA eingefügt; Einordnung von „Nur Erwähnte“-Beiträge im Hinblick auf TK-Dienste und Art. 9-Daten präzisiert; Schwellwertanalyse mit aufgenommen. |
| Anforderungen des DSA mit aufgenommen | Checkliste, Praktische Umsetzung und notwendige Musterdokumente, Muster für ein Impressum | BNetzA als zentrale Kontaktstelle nach dem Digital Services Act mit aufgenommen. |
| Datenschutzhinweise ergänzt | Muster für Datenschutzhinweise | Verarbeitung im Rahmen von Umfragen mit aufgenommen; Rechtsgrundlage für „Nur Erwähnte“-Beiträge präzisiert. |
| Nutzungsbedingungen präzisiert | Muster für Nutzungsbedingungen | Verbleibende Daten bei einer Account-Löschung genauer beschrieben. |

1 Bei der Tabelle handelt es sich nicht um eine vollständige Auflistung der Änderungen. Aufgelistet sind die inhaltlich bedeutsamsten Änderungen im Vergleich zur vorherigen Version.

| Änderung | Positionen im Leitfaden | Erläuterung |
|---|---|---|
| Anforderung einer Schwellwertanalyse mit aufgenommen | Checkliste, Praktische Umsetzung und notwendige Musterdokumente, Verzeichnis von Verarbeitungstätigkeiten und Schwellwertanalyse, Muster für eine Schwellwertanalyse | Notwendigkeit der Durchführung einer Schwellwertanalyse beschrieben; Musterdokument mit Erläuterungen hinzugefügt. |
| Beschreibung des Secure Mode präzisiert | Datenschutzfreundliche Konfiguration eines Mastodon-Servers | Vor- und Nachteile sowie Beschreibung der *Secure-Mode*-Einstellung ausführlicher beschrieben. |
| Umgang mit rechtlichen Unsicherheiten | Checkliste, Praktische Umsetzung und notwendige Musterdokumente | Abschnitt zum Umgang mit rechtlichen Unsicherheiten hinzugefügt. |

# Inhaltsverzeichnis

# Über die Autorinnen

## Jens Kubieziel

Jens Kubieziel engagiert sich seit vielen Jahren in den Bereichen Informationssicherheit, Datenschutz und Anonymität. Im Vorstand des Zwiebelfreunde e.V. betreibt er Tor-Server und unterstützt das Tor-Projekt als Mitglied im Kernteam. Als Datenschutz- oder Informationssicherheitsbeauftragter hilft er Firmen, personenbezogenen Daten und Unternehmenswerte zu schützen. Er nutzt seit über zehn Jahren Dienste des Fediverse, hilft Nutzerinnen bei den ersten Schritten und betreibt mit freie-re.de eine eigene Instanz.

## Malte Engeler

Malte Engeler ist Mitbegründer von „Strukturelle Integrität“, einem radikal bedürfnisorientierten, digitalpolitischen Kollektiv. Er forscht zu Themen des Datenrechts, der postkapitalistischen Datenökonomie und der solidarischen Digitalpolitik. Sein fachlicher Hintergrund liegt in den Rechtswissenschaften.

## Rebecca Sieber

Rebecca Sieber absolviert derzeit die letzte Station ihres Rechtsreferendariats bei der Gesellschaft für Freiheitsrechte e.V., nach Stationen bei der Kanzlei Böhm & Meyer-Dulheuer und der Berliner Beauftragten für Datenschutz und Informationsfreiheit. Seit 2021 untersucht sie die rechtlichen und philosophischen Fragen im Fediverse. Zuvor arbeitete sie als wissenschaftliche Mitarbeiterin an der Humboldt-Universität und an der Freien Universität Berlin und studierte Philosophie im Zweitstudium. Sie engagiert sich seit über zehn Jahren unter anderem für Datenschutz und freie Software.

Die Texte wurden im Auftrag der Stiftung Datenschutz erstellt.

Rebecca Sieber ist Hauptautorin der folgenden Texte:

- „Datenschutzrechtliche Fragestellungen beim Betrieb einer Fediverse-Instanz – am Beispiel von Mastodon“ (begleitend erscheinender wissenschaftlicher Aufsatz)
- Zusammenfassung des begleitend erscheinenden wissenschaftlichen Aufsatzes

Malte Engeler ist Hauptautor der folgenden Texte:

- Praktische Umsetzung und notwendige Musterdokumente
- Muster für ein Impressum, für Datenschutzhinweise und Nutzungsbedingungen

Jens Kubieziel ist Hauptautor der folgenden Texte:

- Anleitung zum Einpflegen von Texten in der Mastodon-Verwaltungsoberfläche
- Datenschutzfreundliche Konfiguration eines Mastodon-Servers
- Muster für ein Verzeichnis der Verarbeitungstätigkeiten und Dokumentation von TOMs
- Muster für eine Schwellwertanalyse
- Informationen für eine Auskunft nach Art. 15 DSVGO

Die Checkliste wurde gemeinsam von Malte Engeler und Jens Kubieziel erstellt.

# Checkliste

## Für alle die sofort loslegen wollen

### Informationspflichten und Vereinbarungen mit Nutzerinnen

- ☐ Hat die Instanz ein Impressum inklusive Angaben zur zentralen Kontaktstelle nach dem Digital Services Act?
- ☐ Sind Datenschutzhinweise hinterlegt?
- ☐ Sind Nutzungsbedingungen hinterlegt?
- ☐ Sind Verhaltensregeln hinterlegt?

### Datenschutz-Management

- ☐ Im Fall eines gehosteten Servers: Wurde ein Auftragsverarbeitungsvertrag mit dem Server-Hoster geschlossen?
- ☐ Wurde das Verzeichnis der Verarbeitungstätigkeiten inklusive einer Schwellwertanalyse und einer Dokumentation der technisch-organisatorischen Maßnahmen erstellt?
- ☐ Wurde gegebenenfalls eine Datenschutzbeauftragte benannt?
- ☐ Ist bekannt, wie Auskunftsrechte und das Recht auf Kopie erfüllt werden?
- ☐ Ist bekannt, welche Datenschutzbehörde zuständig wäre, falls Datenpannen zu melden sind?

### Betriebssystem

- ☐ Regelmäßiges automatisches Backup
- ☐ Test der Wiederherstellbarkeit des Backups
- ☐ Administrationsberechtigung nur für tatsächliche Administratorinnen (sudo, doas etc.)
- ☐ Regelmäßiges Einspielen von Updates
- ☐ Festplattenverschlüsselung eingerichtet
- ☐ Zugang über SSH abgesichert

### Webserver

- ☐ Logging von IP-Adressen deaktiviert
- ☐ TLS eingerichtet
- ☐ Regelmäßige Erneuerung der TLS-Zertifikate eingerichtet

### Technische Konfiguration von Mastodon

- ☐ Speicherung von IP-Adressen deaktiviert
- ☐ Zugang für Administratorinnen über Mehrfaktorauthentisierung

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

## Zusammenfassung des begleitend erscheinenden wissenschaftlichen Aufsatzes

Das Fediverse gilt als datenschutzfreundliche Alternative zu klassischen sozialen Medien wie Twitter oder Facebook. Die dezentrale oder föderale Struktur des Fediverse erschwert Geschäftsmodelle mit personalisierter Werbung. Da im Regelfall freie Software zum Einsatz kommt, kann der Quellcode untersucht und verändert werden. Die Software, zum Beispiel Mastodon, kann auf dem eigenen Server installiert werden, womit man die Kontrolle über die eigenen Daten behalten kann.

Mit dem Wachstum des Fediverse nehmen aber auch die Sorgen über rechtliche Risiken zu. Der Betrieb einer Fediverse-Instanz wirft einige datenschutzrechtliche Fragen auf. Das gilt vor allem, aber nicht nur, wenn Instanzbetreiberinnen Accounts für andere Personen zur Verfügung stellen.

Der wissenschaftliche Aufsatz, welcher begleitend zu diesem Leitfaden erscheint, widmet sich den datenschutzrechtlichen Fragestellungen, die sich bei dem Betrieb einer Mastodon-Instanz ergeben. Er bildet das wissenschaftliche Fundament für die Aussagen des vorliegenden Leitfadens. Der Aufsatz nimmt die Perspektive von privaten Instanzbetreiberinnen ein. Die Fragen, die sich bei dem Betrieb von Instanzen durch öffentliche Einrichtungen oder bei der reinen Nutzung eines Accounts ergeben, werden nur am Rande beleuchtet.

→ **Hier zum wissenschaftlichen Aufsatz**
sds-links.de/mastodon-wissenschaftlicher-aufsatz

### 1. Technische Grundlagen von Mastodon

Mastodon nutzt den ActivityPub-Standard und ergänzt diesen in einiger Hinsicht. Der Activity-Pub-Standard besteht aus einem Client-to-Server- und einem Server-to-Server-Protokoll. Die „MastoAPI“ verwendet nur letzteres. Außerdem verwendet Mastodon HTTP-Signaturen für das Senden (und, wenn der *Secure Mode* aktiviert ist, auch für das Abrufen von Inhalten). Hinzu kommen weitere offene Protokolle wie OAuth oder WebFinger.

Eine Mastodon-Instanz empfängt grundsätzlich alle Inhalte von Account-Inhaberinnen, denen eine Account-Inhaberin der eigenen Instanz folgt. Umgekehrt übermittelt eine Instanz die Beiträge der Account-Inhaberinnen an alle Instanzen, auf denen sich eine Followerin dieser Account-Inhaberin befindet. Daneben gibt es weitere Möglichkeiten, Inhalte von anderen Instanzen einzubinden. Im *Limited Federation Mode* muss die Föderation mit anderen Instanzen erst ausdrücklich bestätigt werden, bevor diese Inhalte der Instanz abrufen können. Öffentliche Inhalte sind aber stets über die Webseite der Instanz öffentlich zugänglich, sofern nicht die Einstellung `DISALLOW_UNAUTHENTICATED_API_ACCESS` aktiviert ist.

## 2. Grundrechtliche Bezüge

Grundrechte richten sich in erster Linie an den Staat. Sie müssen indirekt aber auch bei der Interpretation von Gesetzen berücksichtigt werden. Bei der Auslegung des Digital Services Act (DSA) und der Datenschutz-Grundverordnung (DSGVO) sind die Grundrechte aus der Charta der Grundrechte der Europäischen Union (GrCh) zu beachten. Instanzbetreiberinnen können aber auch unmittelbar an Grundrechte gebunden sein, zum Beispiel bei der Moderation oder bei der Prüfung, ob sie ein berechtigtes Interesse an einer Datenverarbeitung haben.

Ein staatlicher Social-Media-Account ist immer auch mit Eingriffen in Grundrechte verbunden, die gerechtfertigt sein müssen. Staatliche Institutionen sollten möglichst eigene Mastodon-Instanzen betreiben und sich nicht auf Instanzen registrieren, auf die sie nicht ausreichend Einfluss ausüben können.

## 3. Einordnung als digitaler Dienst

Seit dem 17. Februar 2024 haben die allermeisten Instanzbetreiberinnen die neuen Vorschriften für Diensteanbieter nach dem DSA zu beachten. Es ist davon auszugehen, dass auch Mastodon-Instanzen als „digitale Dienste“ anzusehen sind. Damit sind zumindest die Vorschriften für Vermittlungsdienste nach Art. 11-15 DSA, als auch die für Hostingdienste nach Art. 16-18 DSA einzuhalten. Die Pflichten, die sich daraus für Instanzbetreiberinnen ergeben, sind allerdings überschaubar. Das vorgeschriebene Melde- und Abhilfeverfahren ist bei Mastodon bereits eingerichtet. Instanzbetreiberinnen dürfen zudem nicht willkürlich moderieren, sondern müssen sich hierbei an die eigenen Nutzungsregeln halten. Zudem müssen sie Moderationsentscheidungen begründen.

Mit der Geltung des DSA gehen auch Haftungsprivilegien für Instanzbetreiberinnen einher. Für Rechtsverletzungen von Dritten haften sie daher nur, wenn sie Kenntnis von den Inhalten erlangen und nicht unverzüglich tätig werden.

## 4. Adressatinnen datenschutzrechtlicher Pflichten

### 4.1. Anbieterinnen von digitalen Diensten

Instanzbetreiberinnen bieten digitale Dienste an. Damit ist theoretisch das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) anwendbar, vor allem die sogenannte Cookie-Regelung. Die bei Mastodon üblicherweise verwendeten Cookies sind technisch notwendige Cookies. In der Regel ist ein Cookie-Banner daher nicht notwendig. Das ergibt sich aus § 25 Abs. 2 Nr. 2 TDDDG.

### 4.2. Anbieterinnen von Telekommunikationsdiensten

Soweit Beiträge nur für erwähnte Profile sichtbar gemacht werden, könnten Instanzbetreiberinnen auch als Anbieterinnen eines interpersonellen Kommunikationsdienstes angesehen werden. Zumindest im Ergebnis dürften die „direkten Beiträge“ bei Mastodon dem Fernmeldegeheimnis unterliegen. Instanzbetreiberinnen dürfen sich von diesen Inhalten daher grundsätzlich keine Kenntnis verschaffen, sofern es nicht für die Bearbeitung von Meldungen erforderlich ist.

### 4.3. Verantwortlichkeit im Sinne der DSGVO

Die Pflichten aus der DSGVO richten sich in erster Linie an Instanzbetreiberinnen. Sie sind für die Datenverarbeitung „verantwortlich“. Mehrere Stellen können auch gemeinsam verantwortlich sein. In diesem Fall müssen sie nach Art. 26 DSGVO eine transparente Vereinbarung über ihre Aufgabenverteilung treffen.

Im Verhältnis zu anderen Instanzbetreiberinnen sind die Verantwortungsbereiche klar abgegrenzt. Daher sind insbesondere die Betreiberinnen föderierender Instanzen nicht gemeinsam verantwortlich. Auch zwischen Instanzbetreiberin und Account-Inhaberin besteht in der Regel keine gemeinsame Verantwortlichkeit. Sie verfolgen keine gemeinsamen wirtschaftlichen Interessen und schließen keine Verträge über personalisierte Werbung. In der Regel unterliegen Instanzbetreiberinnen auch nicht den Weisungen der Account-Inhaberinnen, sodass in diesem Verhältnis meist kein Auftragsverarbeitungsvertrag zu schließen ist. Ein Fall der Auftragsverarbeitung liegt hingegen vor, wenn Betrieb und Wartung

einer Mastodon-Instanz an eine Dienstleisterin ausgelagert werden oder die Instanzbetreiberin einen (virtuellen) Server mietet.

## 5. Pflichten gegenüber Besucherinnen der eigenen Instanz

Auch das Verwenden und Speichern von technischen Informationen wie IP-Adressen oder der vom User-Agent mitgesendeten Daten ist von der DSGVO erfasst. Instanzbetreiberinnen haben nach Art. 6 Abs. 1 f) DSGVO ein berechtigtes Interesse daran, diese Daten zu erfassen, um die Instanz-Webseite zur Verfügung stellen zu können. Die Log-Dateien des Servers sollten jedoch möglichst kurz oder gar nicht gespeichert werden, um den Grundsätzen der Datenminimierung und der Speicherbegrenzung gerecht zu werden.

## 6. Pflichten gegenüber Account-Inhaberinnen der eigenen Instanz

Bei der Registrierung von Account-Inhaberinnen erheben Instanzbetreiberinnen Bestandsdaten, insbesondere eine E-Mail-Adresse. Außerdem verarbeiten sie Nutzungsdaten wie die IP-Adresse und den Zeitpunkt des Logins. Hinzu kommen die Inhalte, die bei der Interaktion auf einer Mastodon-Instanz gespeichert und an föderierende Instanzen übermittelt werden. Dazu gehören auch die Followerinnen und Follows eines Accounts, die Beiträge, Favorisierungen, „Boosts“ und Antworten auf Umfragen.

Es ist nicht zu empfehlen, für diese Datenverarbeitung eine pauschale Einwilligung einzuholen, indem die Account-Inhaberinnen bei der Registrierung die Datenschutzhinweise akzeptieren müssen. Zumindest die Verarbeitung von Bestandsdaten kann zumeist auf Art. 6 Abs. 1 b) DSGVO gestützt werden. Es kann davon ausgegangen werden, dass es sich bei dem Nutzungsverhältnis um einen „Vertrag“ handelt.

Probleme ergeben sich allerdings bei Informationen, die streng genommen nicht zur Erfüllung des Vertrags erforderlich sind. Zudem können sowohl Bestandsdaten als auch Beiträge sensible Informationen nach Art. 9 Abs. 1 DSGVO enthalten. In diesen Fällen kann davon ausgegangen werden, dass Account-Inhaberinnen mit einer „eindeutigen bestätigenden Handlung“ einwilligen, indem sie diese Informationen im Fediverse teilen. Rechtliche Unsicherheiten für Instanzbetreiberinnen ergeben sich allerdings daraus, dass diese Einwilligung nicht dokumentiert werden kann. Weitere Hürden können sich zudem für Instanzen ergeben, deren thematische Ausrichtung oder Domain-Name schon Rückschlüsse auf sensible Informationen zulässt.

Die meisten der verarbeiteten Daten können von den Account-Inhaberinnen selbst gelöscht werden. Eine Ausnahme gilt möglicherweise für Account-Namen. Diese werden bei Mastodon nicht automatisch gelöscht, damit sie im Anschluss nicht neu vergeben werden können.

## 7. Pflichten gegenüber Account-Inhaberinnen anderer Instanzen

Damit auf einer Instanz auch die Inhalte anderer Instanzen angezeigt werden können, wird in der Datenbank eine Kopie dieser Daten angelegt. Das entspricht auch den Erwartungen der Account-Inhaberinnen anderer Instanzen. Instanzbetreiberinnen haben ein berechtigtes Interesse an diesen Datenverarbeitungen.

Eine Herausforderung kann allerdings darin bestehen, die Auskunftspflichten zu erfüllen. Zum Beispiel könnten andere Account-Inhaberinnen Auskunft darüber verlangen, ob sie betreffende Daten verarbeiten werden. Sie können auch ihr Recht auf Löschung geltend machen, sofern Beiträge nicht automatisiert gelöscht wurden.

## 8. Pflichten gegenüber sonstigen Dritten

Instanzbetreiberinnen verarbeiten in aller Regel auch Informationen über andere Personen. Das ist insbesondere dann der Fall, wenn Account-Inhaberinnen Dritte in ihren Beiträgen erwähnen. In vielen Fällen sind die damit verbundenen Datenverarbeitungen durch die Meinungsfreiheit der Account-Inhaberinnen gerechtfertigt. Es darf sich aber keinesfalls um sensible Informationen handeln, in deren Verbreitung die betroffenen Personen nicht eingewilligt haben oder die sie nicht selbst öffentlich gemacht haben.

Entsprechende Auskunftspflichten sind für Instanzbetreiberinnen schwer zu erfüllen. Sie sind jedenfalls verpflichtet, rechtsverletzende Beiträge auf Anfrage der betroffenen Person zu löschen.

## 9. Organisatorische Pflichten und „Schwellwertanalyse“

Die organisatorischen Pflichten der Verantwortlichen werden vor allem im praktischen Teil dieses Leitfadens dargestellt. Besondere Aufmerksamkeit verdient die Frage, ob die Instanzbetreiberinnen vor Inbetriebnahme eine Datenschutz-Folgen-abschätzung nach Art. 35 DSGVO durchzuführen haben (sog. „Schwellwertanalyse“). Ob die Datenverarbeitungen voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, lässt sich jedoch nicht pauschal beantworten und muss für jede Instanz gesondert beurteilt werden. Hierfür können bestimmte Kriterien herangezogen werden, wovon zumindest ein Kriterium einschlägig sein dürfte, und zwar die Verarbeitung von vertraulichen oder höchst persönlichen Daten.

## 10. Fazit

Grundsätzlich kann eine Mastodon-Instanz datenschutzkonform betrieben werden. Dabei gibt es einige Herausforderungen, insbesondere das Formulieren von vollständigen und korrekten Datenschutzhinweisen. Außerdem muss eine Instanz datenschutzfreundlich und unter Beachtung der IT-Sicherheit konfiguriert werden.

# Praktische Umsetzung und notwendige Musterdokumente

## A. Wichtige Schritte bei der Einrichtung der Instanz

Eine gesetzes- und vor allem datenschutzrechtskonforme Instanz besteht aus zwei Teilen: einer gut aufgestellten Technik und sauberen juristischen Formalitäten. Zum technischen Teil gehören grundlegende Maßnahmen der Datensicherung und der Konfiguration des Servers sowie der Mastodon-Software. Dazu finden sich in nachfolgenden Teilen dieser Handreichung Tipps, Empfehlungen und Musterdokumente. In diesem Kapitel soll es hingegen um die juristisch-formalen Schritte gehen.

Ziel dieser Handreichung ist es, dass die Instanz den gängigen rechtlichen Anforderungen gerecht wird, die im alltäglichen Betrieb zu erfüllen sind. Dazu gehören in jedem Fall die folgenden Teile:

- gesetzliche Pflichtangaben (u.a. das „Impressum“ und Angaben nach dem Digital Services Act),
- ein Auftragsverarbeitungsvertrag (bei Nutzung von Hosting-Diensten),
- die Datenschutzhinweise (teilweise auch „Datenschutzerklärung“ genannt),
- die Nutzungsbedingungen (der „Vertrag“ zwischen Instanzbetreiberinnen und Nutzerinnen) und
- allgemeine Verhaltensregeln („Instanzregeln“ über zulässige Inhalte und Moderation).

Zu allen fünf Themen wird dieser Teil der Handreichung zunächst erklären, worum es dabei geht und welches Ziel damit erreicht werden soll. Dort, wo es möglich ist, stellt diese Handreichung zusätzlich auch Muster bereit oder verweist auf vorhandene Muster. Instanzbetreiberinnen können diese verwenden und gegebenenfalls modifizieren. Außerdem enthält die Handreichung eine Checkliste.

### I. Gesetzliche Pflichtangaben

Bei den gesetzlichen Pflichtangaben geht es im Grunde um in Textform bereitzustellende Informationen, die für alle Personen (mit und ohne Konto auf der Instanz) verfügbar sein müssen, die die Startseite der Instanz aufrufen.

Dazu gehört zuallererst das sogenannte „Impressum“. Die Impressumspflicht war lange im deutschen Telemediengesetz (TMG) geregelt, folgt mittlerweile aber aus den gesetzlichen Vorgaben des Digitale-Dienste-Gesetzes (DDG). Ziel des Impressums ist es, Nutzerinnen von Onlineangeboten (juristisch mittlerweile „Digitale Dienste“ genannt) eine konkrete Ansprechperson zu nennen. Damit soll Menschen die Möglichkeit gegeben werden, sich an eine konkrete Person zu wenden, wenn diese annehmen, dass ihre Rechte beeinträchtigt wurden. Es geht letztlich darum, die Instanzbetreiberinnen – insbesondere für gerichtliche Zustellungen – greifbar zu machen. Diese Pflicht trifft grundsätzlich alle Anbieterinnen von digitalen Diensten (darunter auch Mastodon-Instanzen). Es gibt zwar enge Ausnahmen von der Impressumspflicht. Diese Ausnahmen greifen für den Betrieb von Mastodon-Instanzen aber nur theoretisch. Praktisch müssen alle Instanzen die Impressumspflicht erfüllen.

Was genau in einem Impressum stehen muss, regelt § 5 DDG. Erforderlich sind vor allem der Name der verantwortlichen Personen (mehrere Namen sind möglich), eine Anschrift, weitere elektronische Kontaktmöglichkeiten und eventuell die Angabe gewisser Registerangaben (z.B. Registernummer und -gericht).

Vor allem die Angabe einer Anschrift ist für viele Instanzbetreiberinnen eine Herausforderung, denn vielfach haben die Betreiberinnen keine andere Adresse, über die sie postalisch erreichbar sind, als ihren privaten Wohnsitz. Die möglichen Gefahren, die für bestimmte Personengruppen mit der

Impressumspflicht einhergehen, sind bisher durch die Gesetzgebung leider nicht aufgegriffen worden, so dass das deutsche Recht an dieser Stelle weiter rigoros ist. Das DDG erwartet, dass ein vollständiger Vor- und Nachname angegeben wird. Es muss eine vollständige Anschrift (Postleitzahl, Ort, Straße sowie Hausnummer) genannt werden. Entscheidend ist, dass dort Gerichtspost zugestellt werden kann. Möglichkeiten, die Angabe der eigenen Wohnanschrift zu vermeiden, gibt es nur wenige. Eine Option ist aber, eine bevollmächtigte Person unter einer Büro- oder Firmenanschrift anzugeben. Ein Postfach genügt leider nicht.

**MUSTER FÜR EIN IMPRESSUM**

sds-links.de/mastodon-muster-impressum

Vor- und Nachname
Zustellfähige Adresse
E-Mail-Adresse
Weitere Kontaktmöglichkeit
Vertretungsberechtigte
Umsatzsteueridentifikationsnummer (z. B. USt-ID)
Handelsgericht, Vereinsregister und Registernummer

**Zentrale Kontaktstelle nach dem Digital Services Act:**
Bundesnetzagentur für Elektrizität, Gas, Telekommunikation,
Post und Eisenbahnen
Tulpenfeld 4
53113 Bonn
Telefon: 0228 14-0
Fax: 0228 14-8872
E-Mail: info@bnetza.de
Beschwerdeformular: https://www.dsc.bund.de/DSC/DE/8Formulare/Form06_Beschw/node.html

→ vollständiges Muster auf der Webseite

Zusätzlich müssen zwei unterschiedliche Möglichkeiten zu Kontaktaufnahme angegeben werden. Eine davon muss eine „schnelle elektronische Kontaktaufnahme“ ermöglichen. In der Praxis erfolgt das durch Angabe einer E-Mail-Adresse. Daneben muss eine „unmittelbare Kommunikation“ ermöglicht werden. Dafür wird in der Praxis meist eine Telefonnummer angegeben.

Juristische Personen (Unternehmen, Vereine) müssen darüber hinaus einige weitere Angaben machen, etwa den Namen des Unternehmens, die Rechtsform, die Vertretungsberechtigten und die Registernummer.

Seit Anwendbarkeit des Digital Services Act (DSA) müssen Betreiberinnen von Mastodon-Instanzen (gleiches gilt grundsätzlich für jede Art von Fediverse-Instanz) zusätzlich die „zentrale Kontaktstelle“ (die für die Durchsetzung des DSA zuständige Behörde) nennen und eine direkte Kontaktaufnahme mit dieser Behörde ermöglichen. In Deutschland ist das die Bundesnetzagentur, die über ein Beschwerdeformular erreichbar ist. Auf weitere Pflichten, die aus dem DSA folgen, wird später eingegangen.

Bei Mastodon ist kein spezifischer Ort für den Eintrag dieser Angaben vorgesehen. Es bietet sich daher an, die nötigen Angaben mit der Überschrift „Gesetzliche Pflichtangaben“ in die „Über“-Seite aufzunehmen.

### II. Auftragsverarbeitungsvertrag

Hinter dem juristischen Begriff „Auftragsverarbeitung“ verbirgt sich, was allgemein als IT-Outsourcing bezeichnet wird. Im Falle des Betriebes von Mastodon-Instanzen ist damit der Fall gemeint, dass der physische Server, auf dem die Instanz technisch läuft, nicht selbst betrieben und verwaltet wird, sondern von einer selbstständigen Dritten betrieben wird. Der häufigste Fall einer solchen Auftragsverarbeitung ist die Nutzung von Hostern, die blanke Server bereitstellen und grundlegende technische Leistungen in diesem Zusammenhang anbieten, aber selbst nicht entscheiden, zu welchen Zwecken dieser Server genutzt wird. Den Hostern ist es egal, ob auf dem Server ein Online-Shop, eine Website oder eine Mastodon-Instanz laufen. Sie stellen nur die Mittel bereit und befolgen im Übrigen die Anweisungen der Auftraggeberinnen.

Juristisch nennt man diese Zusammenarbeit eine „Auftragsverarbeitung“. Sie ist dadurch gekennzeichnet, dass eine Seite die Verantwortung dafür trägt, zu welchen Zwecken eine Datenverarbeitungsanlage eingesetzt wird (hier: die Betreiberinnen der Instanz), und die andere Seite nur die technischen Mittel bereitstellt und dabei weisungsabhängig handelt (hier: die Server-Hoster). Die Auftragsverarbeitung ist in Art. 28 DSGVO geregelt. Für dieses Kapitel relevant ist dabei nur, dass die DSGVO dazu verpflichtet, diese Auftragsverarbeitung durch einen Vertrag abzusichern, in dem u. a. geeignete technische und organisatorische Maßnahmen geregelt sind. Diese Auftragsverarbeitungsverträge müssen in der Regel nicht selbst formuliert oder ausgefüllt werden, sondern sind fester Bestandteil der meisten Server-Bereitstellungen von professionellen Hosting-Diensten. Meist werden Details zu den Auftragsverarbeitungsverträgen schon bei der Einrichtung des Servers abgefragt, jedenfalls aber können diese Auftragsverarbeitungsverträge in den Einstellungen oder Kundinnenmenüs der Hoster zusammengeklickt und als PDF o. ä. gesichert werden. Hier muss darauf geachtet werden, dass im Auftragsverarbeitungsvertrag die erforderlichen technischen und organisatorischen Sicherungsvorkehrungen festgehalten sind. Die Auftragsverarbeitung spielt auch in den Datenschutzhinweisen und bei anderen Formalitäten eine Rolle.

**III. Datenschutzhinweise**

Die Datenschutzhinweise (teilweise auch „Datenschutzerklärung“ genannt) sind der dritte elementare Teil einer vorschriftsmäßig betriebenen Instanz. Sie erklären den Nutzerinnen, welche Daten beim Aufruf der Instanz sowie bei der Nutzung des Kontos verarbeitet werden und klären darüber auf, welche Datenschutzrechte die Nutzerinnen haben. Kerninhalte der Datenschutzhinweise sind deshalb eine Darstellung der relevanten Datenverarbeitungen, der rechtlichen Grundlagen für diese Datenverarbeitung sowie die Bezeichnung der Rechte der Nutzerinnen und Angaben über die Verantwortlichkeit für die Datenverarbeitung. Das hier bereitgestellte Muster deckt den Betrieb einer entsprechend dem Kapitel „Datenschutzfreundliche Konfiguration eines Mastodon-Servers“ konfigurierten Instanz ab. Es muss gegebenenfalls angepasst werden, sofern die Instanz anderweitig konfiguriert wird oder weitere Datenverarbeitungen (z. B. Reichweitenmessung) eingebunden werden.

Mastodon sieht für die Datenschutzhinweise eine eigene Unterseite vor. Dort sollten sie auch eingepflegt werden, um ein schnelles Auffinden der Informationen zu ermöglichen.

**MUSTER FÜR DATENSCHUTZHINWEISE**

sds-links.de/mastodon-muster-datenschutzhinweise

Diese Datenschutzhinweise klären darüber auf, welche Informationen bei der Nutzung der Mastodon-Instanz verarbeitet werden und welche Rechte gegenüber den Betreiberinnen der Instanz bestehen. Alle hier dargestellten Ausführungen und die Aufklärung über die Rechte richten sich nach der seit dem 25.05.2018 anwendbaren europäischen Datenschutz-Grundverordnung (DSGVO).

1. Datenverarbeitung bei Aufruf der Startseite, vor der Registrierung und bei jeder Nutzung

Sobald die Startseite der Instanz aufgerufen wird, um sich zu registrieren oder auch während der Nutzung im Allgemeinen, wird eine Verbindung zum Webserver aufgebaut, auf dem diese Instanz betrieben wird. Um dem Browser oder der App auf dem genutzten Endgerät die Inhalte anzeigen zu können, werden dabei entsprechend der verwendeten Protokolle (http, TCP/IP etc.) gewisse Daten verarbeitet. Dazu können gehören:

→ vollständiges Muster auf der Webseite

**MUSTER FÜR NUTZUNGSBEDINGUNGEN**

sds-links.de/mastodon-muster-nutzungsbedingungen

**Ziffer 1**

- Durch Anlegen eines Kontos auf dieser Instanz kommt ein Nutzungsverhältnis zwischen jeder nutzenden Person und den Betreiberinnen der Instanz zustande.
- Für dieses Nutzungsverhältnis gelten die folgenden Bedingungen.

Ziffer 2

- Das Anlegen evines Kontos durch öffentliche Stellen, Behörden oder vergleichbare staatliche Institutionen ist nicht zulässig.

→ vollständiges Muster auf der Webseite

**IV. Nutzungsbedingungen**

Nutzungsbedingungen sind ebenfalls ein Muss. Der Digital Services Act verlangt von allen Betreiberinnen von Mastodon-Instanzen, dass in allgemeinen Geschäftsbedingungen in einfacher Sprache Angaben zu etwaigen Beschränkungen für Nutzerinnen (z. B. zu nicht erlaubten Inhalten) und zur Art der Moderation gemacht werden.

Die Nutzungsbedingungen können darüber hinaus auch juristische Fragen (Kosten der Nutzung, Mindestalter der Nutzerinnen, Gewährleistung bei Fehlern) rund um das rechtliche Verhältnis zwischen Betreiberinnen und Nutzerinnen klären. Die Nutzungsbedingungen legen dabei insbesondere fest, ob die Instanz lediglich als reine Gefälligkeit (keine vertragliche Verbindlichkeit und Haftung, aber auch geringe Zuverlässigkeit für Nutzerinnen) oder als Dienstleistung mit rechtsgeschäftlichem Bindungswillen (gegenseitige vertragliche Rechte und Pflichten, größere Zuverlässigkeit für Nutzerinnen) angeboten und betrieben wird. Abhängig von den Umständen und der Dauer des Betriebes der Instanz können die Nutzungsverhältnisse vertraglichen Charakter erhalten. Entscheidend ist dabei nicht die Einordnung durch die Instanzbetreiberinnen selbst, sondern wie die Bedingungen für die Nutzung auf objektive Dritte wirken.

Dass die Nutzung der Instanz kostenfrei ist, heißt beispielsweise nicht, dass der Betrieb damit in jedem Fall als reine Gefälligkeit einzuordnen ist. Stattdessen kann je nach erwecktem Eindruck auch ein sogenanntes Gefälligkeitsverhältnis vorliegen, der zwar weniger Rechte und Pflichten erzeugt als ein normaler rechtsgeschäftlicher Dienstleistungsvertrag, aber – anders als die reine Gefälligkeit – doch gewisse wechselseitige Ansprüche auslöst. Es ist grundsätzlich ratsam, bei einer öffentlichen und auf Dauer betriebenen Instanz davon auszugehen, dass mindestens ein solches rechtsgeschäftsähnliches Gefälligkeitsverhältnis vorliegt. Dies sollte sich in den Nutzungsbedingungen widerspiegeln und wird dem beigefügten Muster zugrunde gelegt. Die Nutzungsbedingungen sind zu guter Letzt auch (mittelbar) für die in der Datenschutzerklärung anzugebenden Rechtsgrundlagen von Bedeutung.

Die Mastodon-Software sieht für Nutzungsbedingungen keinen eigenen, speziellen Ort vor. Die Nutzungsbedingungen müssen also anderswo eingefügt werden. Da die Nutzungsbedingungen eine gewisse Relevanz für die Datenschutzhinweise haben, wird hier vorgeschlagen, sie ebenfalls in die „Datenschutzerklärung“-Unterseite einzutragen.

**V. Verhaltensregeln**

Verhaltensregeln (teilweise auch „Code Of Conduct“ oder „Netiquette“ genannt) dienen dazu, die Atmosphäre und die allgemeinen Umgangsformen auf einer Instanz zu gestalten. Inhaltlich beschreiben sie vor allem, welche Inhalte und Umgangsformen auf der Instanz nicht erwünscht sind und gegebenenfalls Sanktionen mit sich bringen können. Die Mastodon-Software sieht für Verhaltensregeln unter dem Menüpunkt „Serverregeln“ als Teil des Administrationsbereichs einen eigenen Ort vor. Diese Handreichung formuliert die Verhaltensregeln deshalb von den Nutzungsregeln getrennt und empfiehlt, sie an vorgesehener Stelle separat einzufügen. Rechtlich sind sie aber Teil der Nutzungsbedingungen und sind spätestens seit Geltungsbeginn des DSA auch zwingend Teil jeder Selbstbeschreibung einer Instanz.

Der Inhalt der Verhaltensregeln ist sehr abhängig davon, an wen sich die Instanz richtet und welche Themen dort im Mittelpunkt stehen. Es wird deshalb auf die Bereitstellung eines Musters verzichtet.

Es wird aber empfohlen, mittels Verhaltensregelung darauf hinzuwirken, dass sich auf der Instanz

Menschen mit vielfältigen politischen, religiösen oder sexuellen und geschlechtlichen Einstellungen sowie Identitäten willkommen fühlen und insbesondere Hass und digitale Gewalt gegen Menschen abseits der Mehrheitsgesellschaft keinen Raum haben. Wenn das Fediverse langfristig ein Safe Space sein soll, braucht es sowohl ein klares Bekenntnis zu Vielfalt als auch konkretes Vorgehen gegen jene, die diese Vielfalt – oft auch im Namen der Neutralität – missachten. Daneben empfehlen sich allgemeine Aussagen dazu, ob Bots auf der Instanz erlaubt sind und ob oder in welcher Form bezahlte Beiträge (Sponsoring, Werbung) zulässig sein sollen. In den Verhaltensregeln sollte auch eine grundsätzliche Aufklärung darüber enthalten sein, dass Inhalte gemeldet werden können und von Moderatorinnen überprüft werden. Dabei empfehlen wir aber, auch deutlich zu machen, dass – der Dezentralität des Fediverse geschuldet – die Moderatorinnen einer Instanz bei Konten anderer Instanzen weniger Möglichkeiten haben als bezüglich Konten der eigenen Instanz.

## B. Pflichten während des Betriebs einer Instanz

Neben den rechtlichen Basics, die mit den genannten Formalitäten vor Start jeder Instanz abgedeckt werden müssen, gibt es auch im laufenden Betrieb einige Pflichten oder jedenfalls Empfehlungen.

### I. Pflichten nach dem Digital Services Act

Der Digital Services Act (DSA) ist ein europäisches Gesetz, in dem geregelt wird, wofür digitale Dienste haften, welche Inhalte zulässig sind und wie diese Inhalte moderiert werden müssen. Der DSA hatte bei seiner Entstehung große, kommerzielle Dienste und Plattformen im Blick und sieht für diese umfangreiche und komplexe Pflichten vor. Grundsätzlich findet der DSA auch auf Mastodon-Instanzen Anwendung. Das Fediverse, seine dezentrale Natur und ehrenamtlich betriebenen Kleinstinstanzen sind allerdings nicht gesondert bedacht worden. Es gibt aber immerhin in Artikel 19 des DSA viele Erleichterungen für Kleinst- oder Kleinunternehmen. Für sie gilt nur ein überschaubarer Teil der vielen Pflichten des DSA. Kleinst- und Kleinunternehmen sind Unternehmen, die weniger als 10 bzw. 50 Personen beschäftigen und weniger als 2 Millionen Euro bzw. 10 Millionen Euro an Umsatz erwirtschaften.

Die allermeisten Fediverse-Instanzen beschäftigen zwar unter 50 Personen (wenn überhaupt) und verbuchen meist auch keinerlei bis kaum Umsatz. Das Problem ist allerdings, dass sie nicht von „Unternehmen“, egal welcher Größe, betrieben werden. Stattdessen sind es oft Einzelpersonen, kleine Gruppen von Menschen und ehrenamtlich Aktive, die diese Instanzen betreiben. Seltener sind es auch mal eingetragene Vereine. Juristisch lässt sich gut vertreten, dass diese kleinen nicht-unternehmerischen Instanzen durch Artikel 19 des DSA in gleicher Weise wie Kleinst- oder Kleinunternehmen vom Großteil der Pflichten des DSA ausgenommen sind. Trotzdem gibt es hier eine Restunsicherheit. Im Zweifelsfall ist nicht mit letzter Sicherheit absehbar, ob die nationalen Aufsichtsbehörden oder die Europäische Kommission Mastodon-Instanzen tatsächlich als „Kleinst- oder Kleinunternehmen“ im Sinne des Artikel 19 des DSA behandeln werden. Es ist zwar kaum zu erwarten, dass die Behörden Mastodon-Instanzen besonders ins Visier nehmen oder ihnen das Leben schwer machen werden. Ein Restrisiko geht mit dem Betrieb von Instanzen bis zu einer Klärung dieser Rechtsfrage dennoch einher.

Geht man davon aus, dass die Erleichterungen des Artikel 19 des DSA auch für Mastodon-Instanzen gelten, müssen Betreiberinnen im laufenden Betrieb lediglich folgende Pflichten erfüllen:

1. Gemäß Artikel 16 DSA müssen Nutzerinnen Inhalte, die sie als rechtswidrig ansehen, mit leicht zugänglichen und benutzerfreundlichen Verfahren melden können. Betreiberinnen von Instanzen müssen diese Meldungen zeitnah bearbeiten.

2. Instanzbetreiberinnen müssen auf Meldungen reagieren, angemessene Maßnahmen ergreifen und diese Maßnahmen gegenüber den Betroffenen begründen (Artikel 17 und 18 DSA).

3. Erhalten Instanzbetreiberinnen Kenntnis von Informationen, die den Verdacht begründen, dass bestimmte schwere Straftaten begangen wurden oder begangen werden könnten, müssen die Strafverfolgungs- oder Justizbehörden informieren werden (Artikel 18 DSA).

4. Instanzbetreiberinnen müssen mindestens alle sechs Monate öffentlich mitteilen, wie viele aktive Nutzerinnen die Instanz hat. Auf Anfrage ist dies auch im Einzelfall den Behörden mitzuteilen (Artikel 24 Absatz 2 und 3 DSA).

Die nötigen Werkzeuge für die Umsetzung dieser Pflichten liefert Mastodon über die integrierten Melde- und Moderationswerkzeuge mit. Auch die Angabe der aktiven Nutzerinnen ist eine standardmäßig verfügbare Funktion. Es geht bei diesen Pflichten also vor allem darum, diese vorhandenen Werkzeuge auch gewissenhaft und bewusst zu nutzen.

**II. Verzeichnis von Verarbeitungstätigkeiten und Risikobewertung**

Wer eine Mastodon- oder Fediverse-Instanz betreibt und personenbezogene Daten verarbeitet, sollte sogenannte Verzeichnisse von Verarbeitungstätigkeiten anlegen und aktualisieren. Die DSGVO versteht darunter eine jederzeit für die Datenschutzaufsichtsbehörde verfügbare Dokumentation der wesentlichen Datenverarbeitungen. Diese Dokumentation ist in Art. 30 DSGVO geregelt. Demnach müssen alle Verantwortlichen ein Verzeichnis aller Verarbeitungstätigkeiten führen, die ihrer Zuständigkeit unterliegen. In diesem Verzeichnis sind u.a. Daten zu den Verantwortlichen, die Zwecke der Verarbeitung, eine Beschreibung der verarbeiteten Daten(kategorien) und Empfängerinnen dieser Daten aufzuführen. Ein teilweise vorausgefülltes Muster steht im Kapitel „Verzeichnis von Verarbeitungstätigkeiten“ zur Verfügung. Es genügt, das Verzeichnis elektronisch zu speichern und – gegebenenfalls – der Aufsichtsbehörde zur Verfügung zu stellen. Der Inhalt des Verzeichnisses sollte regelmäßig auf Aktualität überprüft werden.

Es kann sein, dass bestimmte Verarbeitungsvorgänge ein voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen. Finden derartige Risikoverarbeitungen während des Betriebs einer Mastodon-Instanz statt, ist vor Beginn der Datenverarbeitung eine sogenannte „Datenschutz-Folgenabschätzung“ gemäß Art. 35 DSGVO durchzuführen. Dabei handelt es sich um einen bestimmten formalisierten Prozess, mit dem nachweisbar ermittelt werden soll, dass die Risiken angemessen eingeschätzt wurden und die erforderlichen Maßnahmen zur Bewältigung der Risiken getroffen wurden. In der Regel dürfte eine solche Datenschutz-Folgenabschätzung für den Betrieb einer Mastodon-Instanz nicht erforderlich sein. Im Einzelfall und je nach inhaltlicher Ausrichtung der Instanz kann sie aber notwendig werden. Deshalb soll an dieser Stelle kurz darauf eingegangen werden.

Die DSGVO enthält nur allgemeine Hinweise dazu, wann Verfahren ein so hohes Risiko mit sich bringen, dass eine Datenschutz-Folgenabschätzung geboten ist. Die Datenschutzaufsichtsbehörden haben deshalb Kriterienkataloge entwickelt, damit Verantwortliche analysieren können, wann die eigene Datenverarbeitung die Schwelle zur Pflicht einer Datenschutz-Folgenabschätzung überschreitet. Im Rahmen dieser Schwellenwertanalyse gibt es verschiedene Kriterien, die als Indikatoren herangezogen werden. Im wissenschaftlichen Aufsatz, der als eigenständiger Text zu diesem Leitfaden gehört, sowie in dem Muster der Schwellwertanalyse, werden diese Kriterien erörtert und beispielhaft für Mastodon-Instanzen bewertet.

**III. Datenschutzbeauftragte**

Die DSGVO sieht als begleitende Schutzmaßnahme vor, dass Verantwortliche eine Datenschutzbeauftragte benennen können. Diese beauftragte Person unterstützt die Verantwortlichen dabei, sich datenschutzkonform zu verhalten, ist aber nicht selbst verantwortlich im Sinne des Datenschutzrechts. Sie ist unabhängig und hinsichtlich ihrer Tätigkeit nicht weisungsgebunden. Rechtlich ist die Benennung einer solchen Person (außerhalb von Behörden) nach Art. 37 DSGVO nur verpflichtend, wenn die Datenverarbeitung besonders sensibel ist oder wenn in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind (§ 38 BDSG). Bezüglich Mastodon-Instanzen dürften derzeit – wenn überhaupt – nur sehr wenige große und professionell betriebene Instanzen unter die Pflicht zur Benennung fallen. Trotzdem kann es auch bei kleineren Instanzen – etwa bei solchen, die durch Vereine oder Interessengemeinschaften betrieben werden – sinnvoll und hilfreich sein, eine Datenschutzbeauftragte zu benennen, um bei dieser Person Sachverstand und Aufgaben zu bündeln. Wird eine Datenschutzbeauftragte benannt, muss diese auch in den Datenschutzhinweisen angegeben werden.

## C. Besondere Situationen und die Reaktion darauf

Auch wenn die Instanz formal und technisch rechtskonform eingerichtet wurde, kann es im laufenden Betrieb Handlungsbedarf geben. Die häufigsten Situationen sind dabei, dass Personen ihre Rechte auf Auskunft und Kopie geltend machen oder dass eine Datenpanne passiert.

**I. Auskunftsverlangen**

Der praktisch häufigste Fall dürfte sein, dass Personen die Instanzbetreiberinnen kontaktieren und Auskunft über die auf der Instanz über sie verarbeiteten Daten verlangen. Das Auskunftsrecht gehört zu den zentralen Betroffenenrechten und verpflichtet Verantwortliche dazu, den Betroffenen eine Vielzahl an Informationen bereitzustellen. Nach Art. 15 DSGVO und für die Zwecke dieser Handreichung besonders relevant sind:

- die Verarbeitungszwecke;
- die Kategorien personenbezogener Daten, die verarbeitet werden;
- die Empfängerinnen oder Kategorien von Empfängerinnen, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängerinnen in Drittländern oder bei internationalen Organisationen;
- falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten.

Solche Anfragen sind jederzeit und ohne weitere Voraussetzungen möglich. Insbesondere muss kein „guter Grund“ für ein Auskunftsverlangen angegeben werden. Eine Antwort kann in der Regel auch nicht damit verweigert werden, dass das Zusammenstellen der nötigen Informationen Mühe macht oder Zeit kostet. Tatsächlich entsprechen viele der gesetzlich vorgeschriebenen Informationen aber den Informationen, die gleichzeitig auch in den Datenschutzhinweisen und dem Verzeichnis über die Verarbeitungstätigkeiten enthalten sind.

Der EuGH hat Anfang 2023 entschieden, dass in der Regel nicht nur die Kategorien von Empfängerinnen beauskunftet werden müssen, sondern auch die konkreten Empfängerinnen selbst. Im Rahmen des Betriebs einer Mastodon-Instanz dürfte sich dies trotzdem auf die Angabe beschränken, dass die Daten aus den Beiträgen grundsätzlich an alle föderierten Instanzen übermittelt werden, während die nicht-öffentlichen Daten nur mit dem Server-Hoster im Rahmen einer Auftragsverarbeitung geteilt werden.

Bezüglich der verarbeiteten Daten genügt die Angabe von Datenkategorien (etwa: Informationen aus der Registrierung und Inhalt von Beiträgen). Dies ist insbesondere relevant, wenn Personen Auskunft begehren, die kein Konto auf der Instanz haben. Auch diese haben einen Anspruch auf Auskunft darüber, welche Informationen über sie auf der Instanz gespeichert sind. Diese verbergen sich aber grundsätzlich potenziell in einer Vielzahl von Beiträgen, in denen über diese Person eventuell gesprochen wurde. Hier muss dennoch nicht der Inhalt aller entsprechenden Beiträge durchsucht und beauskunftet werden, sondern nur die Kategorie (Informationen in Beiträgen von Nutzerinnen) angegeben werden. Eine Auskunftserteilung ist insgesamt also keine unlösbare Herausforderung.

**II. Recht auf Kopie**

Das Recht auf Kopie ist in Art. 15 Abs. 3 DSGVO geregelt und räumt das Recht ein, nicht nur Auskunft über die grundsätzliche Datenverarbeitung zu erhalten, sondern eine Kopie der konkreten Daten selbst. Dieses Recht beschränkt sich nicht auf Kategorien von Daten, sondern verleiht laut EuGH ein Recht auf eine originalgetreue und verständliche Reproduktion der Daten. Praktisch empfiehlt sich hier, die Nutzerinnen auf die Möglichkeit zu verweisen, ihr Archiv herunterladen. Diese Möglichkeit räumt Mastodon allen Nutzerinnen in den Einstellungen ein. Das Recht erfasst grundsätzlich aber auch eine Kopie aller sonstigen Daten, die in den Mastodon-Datenbanken gespeichert sind. Im Kapitel „Informationen für eine Auskunft nach Art. 15 DSVGO“ sind Tipps zu finden, wie dem Recht auf Kopie insoweit genüge getan wird.

Anders als das Recht auf Auskunft steht das Recht auf Kopie unter dem Vorbehalt, dass es Rechte und Freiheiten anderer Personen nicht beeinträchtigt (Art. 15 Abs. 4 DSGVO). Das Recht auf Kopie muss nach überwiegender Lesart deshalb nur erfüllt werden, wenn es unter Abwägung mit den Rechten anderer Nutzerinnen und auch der Instanzbetreiberinnen erfüllbar ist. Die Anforderung einer Kopie ist in der Regel mit verhältnismäßigem Aufwand erfüllbar, wenn sie von Nutzerinnen der Instanz

ausgehen. Kommen sie hingegen von Personen, die kein Konto auf der Instanz haben, wird es deutlich schwerer. Grundsätzlich müsste hier eine Volltextsuche über sämtliche Informationen der Mastodon-Instanz stattfinden und alle direkt oder indirekt auf die jeweilige Person beziehbaren Informationen in Kopie bereitgestellt werden. Hier dürfte die Grenze der Verhältnismäßigkeit schnell erreicht sein, da es den Betreiberinnen einer Instanz angesichts der üblicherweise begrenzten technischen Mittel nur schwer möglich ist, den Inhalt aller Beiträge kontextabhängig darauf zu untersuchen, ob über die Person gesprochen wurde, die eine Kopie fordert. Gegenüber Personen, die kein Konto auf der Instanz haben, dürfte das Verlangen nach einer Kopie in der Regel also oft abgelehnt werden können.

**III. Datenpannen**

Selbst den gewissenhaftesten Betreiberinnen von Instanzen können Fehler passieren, oder es ist einfach Pech (etwa wenn nicht bekannte Sicherheitslücken ausgenutzt wurden). Wenn beim Betrieb einer Instanz Daten an Unbefugte gelangen oder allgemein die Datenschutzrechte von Personen verletzt werden, verpflichtet Art. 33 DSGVO dazu, grundsätzlich binnen 72 Stunden Meldung bei der Datenschutzbehörde und im Falle besonderer Risiken für Personen nach Art. 34 DSGVO auch gegenüber den Betroffenen zu machen. Viele Aufsichtsbehörden haben dafür ein Online-Formular auf ihrer Webseite. Details zur Meldung von Datenpannen finden sich im Kapitel „Datenschutzfreundliche Konfiguration eines Mastodon-Servers". Grundsätzlich sollte hier jedoch keine Sorge vor nachteiligen Folgen bestehen. Soweit die Instanz technisch sauber betrieben wird, alle nötigen Sicherheitsupdates installiert waren und die hier genannten Formalitäten eingehalten wurden, ist es sehr unwahrscheinlich, dass es Ärger mit der Datenschutzaufsicht gibt.

**IV. Pragmatischer Umgang mit Rechtsunsicherheiten**

Der Betrieb von Mastodon-Instanzen ist kein juristisches Wagnis. Im Detail gibt es aber rechtliche Unklarheiten, die auch diese Handreichung nicht ohne Weiteres auflösen kann. Die größten Unsicherheiten sind die Pflichten des Digital Services Act und das Posten von sensiblen Daten in Posts mit beschränkter Öffentlichkeit. Bei ersterem ist offen, ob die Erleichterungen für kleine Unternehmen auch für Instanzen gelten. Bei zweiterem ist offen, ob das aktive Veröffentlichen sensibler Inhalte als Einwilligung im Sinne der DSGVO gewertet werden kann. Für derartige Unsicherheiten gibt es keine perfekten Lösungen.

Grundsätzlich können sich Nutzerinnen oder sonstige Personen jederzeit über (behauptete) Rechtsverstöße auf Fediverse-Instanzen bei den zuständigen Aufsichtsbehörden beschweren. Die Behörden können auch ohne Beschwerde von Amts wegen tätig werden, wenn es dafür sachliche Gründe gibt. Dabei gilt: Die Datenschutzaufsichtsbehörden sowie die Bundesnetzagentur sind Teil des staatlichen Gewaltmonopols. Grundsätzlich sind sie es also, die sich für Maßnahmen gegenüber Betreiberinnen von Mastodon-Instanzen rechtfertigen müssen. Gleichzeitig sind die Behörden von Gesetzes wegen verpflichtet, auf Beschwerden hin tätig zu werden. Sie haben dafür diverse rechtliche Befugnisse, von Fragerechten bis hin zum Recht, Datenverarbeitungsanlagen (z.B. den Server, auf dem die Instanz läuft) vor Ort zu prüfen. Bisher gibt es wenig Grund für die Annahme, dass die Behörden den Betrieb von Mastodon-Instanzen für besonders problematisch halten oder gar schwerpunktmäßig Prüfungen in diesem Bereich vornehmen. Schließlich unterhalten die Behörden oft selbst Konten auf einer Instanz oder betreiben diese gar selbst. Es spricht Einiges dafür, dass die Aufsichtsbehörden, jedenfalls bei erstmaligem Kontakt zwischen Instanzbetreiberinnen und Behörde, versuchen werden, ein Verfahren niederschwellig und eher beratend zu lösen, statt direkt Sanktionen zu verhängen. Denkbar ist auch, dass die Behörde eine Instanzbetreiberin dazu verpflichtet, bestimmte Änderungen vorzunehmen, die bisher versäumt wurden.

Instanzbetreiberinnen sollten mit dieser Situation so umgehen, dass sie die in dieser Handreichung beschrieben formalen und juristischen Empfehlungen (z.B. Verfahrensverzeichnisse anlegen, Schwellwertanalyse durchführen und Datenschutzhinweise anpassen) umsetzen und sich darüber hinaus auf dem Laufenden halten, was rechtliche Änderungen betrifft.

## D. Anleitung zum Einpflegen von Texten in der Mastodon-Verwaltungsoberfläche

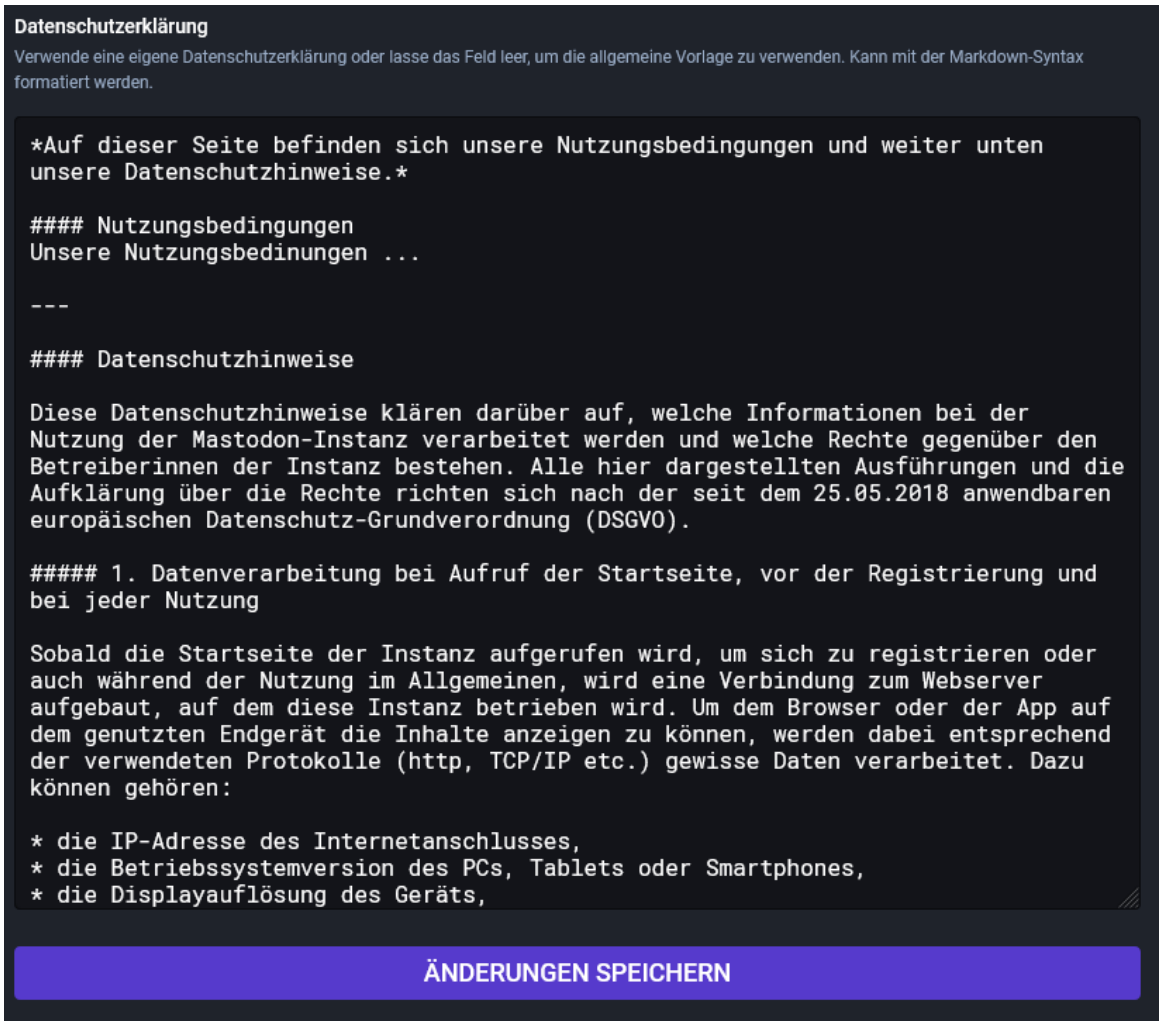
Die Weboberfläche von Mastodon bietet im Administrationsbereich verschiedene Eingabefelder, an denen die rechtlich notwendigen Pflichtangaben öffentlich einsehbar hinterlegt werden können. Es gibt derzeit jedoch keine getrennten Bereiche für Impressum, Datenschutzhinweise und Nutzungsbedingungen, so dass eine „kreative“ Nutzung der vorhandenen Felder notwendig ist.

Um die Texte in die vorhandenen Felder einzufügen, bietet sich das folgende Vorgehen an:

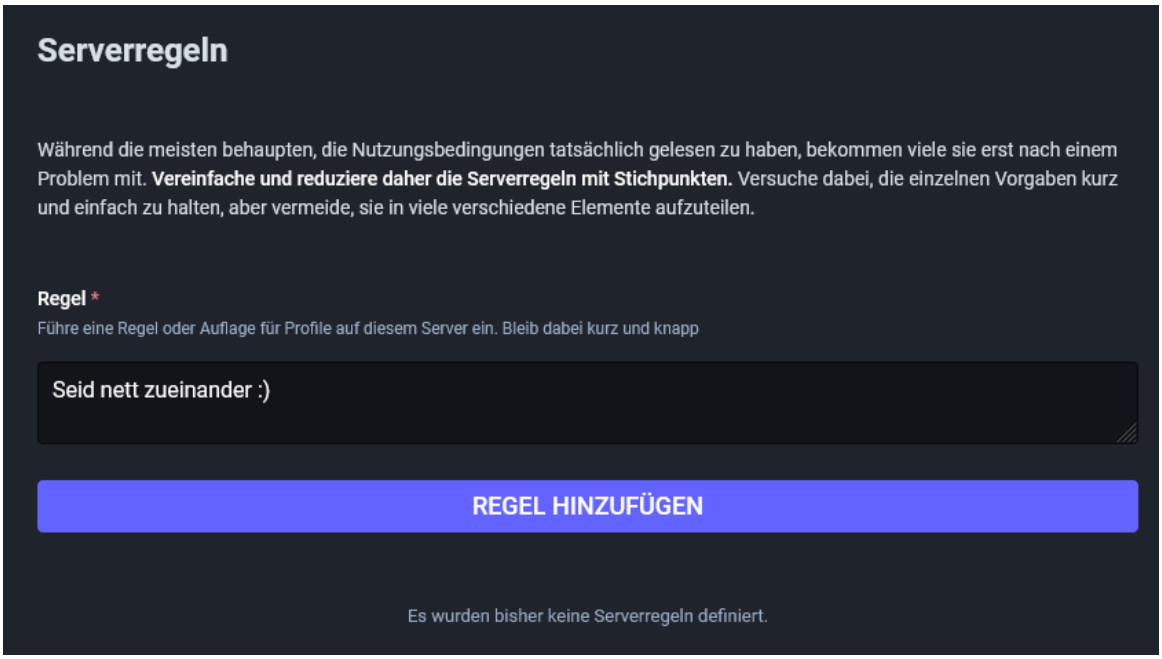
Im angemeldeten Zustand befindet sich als Administrator unter Einstellungen der Administrationsbereich. Dort gibt es unter den Servereinstellungen zwei Textfelder im Bereich Über, die man mit längeren Markdown-formatierten Texten füllen kann.

Das obere Feld Erweiterte Beschreibung ist für die unter /about abrufbare Serverbeschreibung gedacht. Da die Seite über den Link mit der Bezeichnung Über von allen Unterseiten aus aufrufbar ist, kann man hier zusätzlich das Impressum platzieren:

Der Text aus dem unteren Feld Datenschutzerklärung wird unter /privacy-policy angeboten und ist von allen Unterseiten aus über einen Link mit der Bezeichnung Datenschutzerklärung aufrufbar. Zusätzlich wird die Seite über eine Checkbox aktiv in den Registrierungsprozess einbezogen, so dass sich dieser Bereich für das Hinterlegen von Nutzungsbedingungen und Datenschutzhinweisen auf einer Seite eignet:



Daneben gibt es außerdem den Bereich Server-regeln, welcher ein direkter Menüpunkt unterhalb von Administration ist. Die Serverregeln müssen in einzelnen Feldern angegeben werden und sind auf der /about-Seite in einem aufklappbaren Bereich mit eingebunden. Wie zuvor erläutert, eignet sich dieser Bereich für die Platzierung der Verhaltens-regeln bzw. eines Code of Conduct:



# Datenschutzfreundliche Konfiguration eines Mastodon-Servers

Das folgende Kapitel beschreibt eine Konfiguration eines Mastodon-Servers mit besonderem Schwerpunkt auf einer datenschutzfreundlichen Konfiguration.

Sehr viele Privatpersonen, Vereine oder kleine Firmen haben sich auf den Weg gemacht, um das Fediverse durch den Betrieb eines Mastodon-Servers zu unterstützen. Hierbei greifen sie im Rahmen ihrer Möglichkeiten auf bestimmte Ressourcen zurück. Das heißt, einige nutzen die Dienste eines Rechenzentrums. Die Server stehen dort zusammen mit anderen in klimatisierten Räumen, in denen Zugänge zu einzelnen Maschinen genau geregelt sind. Andere betreiben den Server in Wohn-, Vereins- oder auch in Firmenräumen. Dort sind die allgemeinen Umstände viel weniger geregelt. Die Spannweite reicht von allgemein zugänglichen Räumen bis zu einem eigenen kleinen Serverraum.

Daher versucht der Leitfaden auf verschiedene Bedürfnisse einzugehen und hierfür Rat anzubieten. Dies geht an einigen Stellen zu Lasten der Konkretheit. Es wurde jeweils versucht, die allgemeine Vorgehensweise zu beschreiben und dann möglichst konkrete Hinweise zu geben.

## 1. Einleitung

Für das vorliegende Kapitel wird angenommen, dass alle Software auf einem Linux-basierten System installiert und betrieben wird. Die Tests der vorgestellten Einstellungen erfolgten auf Basis der Distribution Debian GNU/Linux. Sofern konkrete Pfade zu Dateien oder Verzeichnissen genannt werden, kann es bei anderen Distributionen teils Abweichungen geben.

## 2. Software für den Betrieb von Mastodon

Neben dem Betriebssystem benötigt Mastodon weitere Software, um korrekt betrieben werden zu können. Dazu gehören:

- Mailserver
- Webserver (nginx)
- Datenbank-Management-System (PostgreSQL)
- weitere Software (Ruby, Node.js etc.)

### 2.1 Mailserver

Ein korrekt eingerichteter Mailserver mit allen Komponenten wird für dieses Kapitel vorausgesetzt. Dabei sei auf die Anleitung von Thomas Leister[1] verwiesen. Diese beschreibt alle notwendigen Schritte für den sicheren Betrieb eines Mailservers.

### 2.2 Webserver

Die Entwicklerinnen von Mastodon gehen davon aus, dass nginx als Webserver verwendet wird und liefern bereits eine Konfigurationsdatei mit aus. Daher wird im folgenden nur nginx als Software für den Webserver betrachtet. Auf andere Webserver soll nicht eingegangen werden.

### 2.3 Datenbank-Management-System

Die Mastodon-Software nutzt ein Datenbank-Management-System (DBMS), um Daten dort abzulegen oder abzurufen. Die Entwicklerinnen haben sich für das DBMS PostgreSQL entschieden. Mögliche sinnvolle Einstellungen werden in Abschnitt „Einstellungen für den Datenbank-Server“ beschrieben.

1 Mailserver mit Dovecot, Postfix, MySQL und Rspamd unter Debian 11 Bullseye / Ubuntu 22.04 LTS

## 3. Allgemeine Betrachtungen zur Sicherheit des Mastodon-Servers

Bevor genauere Einstellungen des Servers diskutiert werden, sollen zunächst einige allgemeine Überlegungen hinsichtlich der IT- bzw. Informationssicherheit des Servers angestellt werden. Sowohl die Grundsätze der DSGVO wie auch der Artikel 32 der Grundverordnung fordern angemessene Sicherheitsmaßnahmen bei der Verarbeitung personenbezogener Daten. Einige Überlegungen hinsichtlich der Informationssicherheit sollen unten diskutiert werden.

### 3.1 Zugang zum Server

Angriffe, die nicht in die Nähe eines IT-Systems kommen, können natürlich auch keinen Schaden anrichten. Maßnahmen zur Zugangskontrolle versuchen genau dies sicherzustellen.

Im Allgemeinen ist es empfehlenswert, den Server bei einem Provider mit entsprechenden Garantien zu betreiben. Viele professionelle Provider sind zertifiziert nach ISO/IEC 27001 bzw. ähnlichen Standards und sichern über Auftragsverarbeitungsverträge zu, wer Zugang zum Server hat und wie die Maßnahmen zur Zugangskontrolle gestaltet sind. Damit haben die Betreiberinnen des Mastodon-Servers einfache und klare Informationen, wer Zugang zu deren Servern hat.

Falls der Server außerhalb eines solchen Rechenzentrums betrieben werden sollte, ist viel mehr Augenmerk auf den Zugang zum Server zu legen. Die Spannbreite kann hier von einem Rechner liegen, der innerhalb eines Vereins, einer gemeinsamen Wohnung oder Ähnlichem betrieben wird, bis hin zu einem Server, der innerhalb eines Serverraums mit klaren Regeln steht. Dies macht es schwer, einen allgemeinen Rat zu geben.

Eine Betreiberin eines Servers sollte sich daher immer die Frage stellen, wem der Zugang zu dem Server möglich ist und wie der Zugang von unbefugten Personen verhindert werden kann. Das heißt, mögliche Maßnahmen wären

- abgeschlossene Räume (Türen, Fenster etc.),
- klare Regelungen und Kontrolle, wer Zugang zu diesen Räumen hat,
- Einsatz von Alarmanlagen.

Daneben lassen sich weitere Maßnahmen denken, die abhängig vom jeweiligen Ort sind. Hinsichtlich der Zugangskontrolle sollten sich diese eignen, Angreiferinnen von den IT-Systemen fern zu halten. Hier wie auch bei anderen Sicherheitsmaßnahmen ist eine gestaffelte Vorgehensweise sinnvoll und wichtig. Das bedeutet, selbst wenn eine Angreiferin es geschafft hat, eine Hürde zu überwinden, gibt es weitere Schutzmaßnahmen, die es zu überwinden gilt.

Beispielsweise könnte jemand auf die Idee kommen, die „sicherste Tür der Welt“ einzubauen und auf deren Sicherheitsgarantien zu vertrauen. Nichtsdestotrotz könnte ein Wachdienst helfen, Angreiferinnen von der Tür fernzuhalten. Weiterhin wäre eine Alarmanlage sinnvoll. Diese könnte für den Fall aktiv werden, dass das Sicherheitsversprechen der Tür versagt.

### 3.2 Zugriff auf die Daten

Wenn der Zugangsschutz als erste Hürde versagt, wäre ein Angreifer in der Lage, den Server für seine Zwecke zu verwenden bzw. zu missbrauchen. Daher sind Maßnahmen zum Zugriffschutz die nächste Hürde, die hier wirksam wird. Der Zugriff auf die Daten, insbesondere auf die personenbezogenen Daten, soll nur befugten Personen möglich sein. Damit sind Maßnahmen zu planen, die den Zugriff auf diese Daten schützen.

Einerseits kann man sich Angreifer vorstellen, die in die Räumlichkeiten einbrechen bzw. mutwillig Zugangshürden überwinden. Andererseits sind auch Personen vorstellbar, die Zugangsrechte haben und nicht auf die Daten zugreifen sollen. Typischerweise sind Reinigungs-oder Reparaturdienste in einer solchen Position. Aber auch Besucherinnen, Gäste oder Nutzerinnen, die nicht den Mastodon-Server administrieren sollen, gehören dazu.

Diese Maßnahmen umfassen sichere Authentifizierung durch den Server. Das bedeutet, der Server muss in der Lage sein zu verifizieren, dass die richtige Person versucht, auf die Daten zuzugreifen. Sinnvolle Mittel sind

- sichere Passwörter
- Mehrfaktorauthentisierung
- Verwendung von Schlüsseln oder Zertifikaten bei der Administration über SSH oder andere Remote-Administrationswerkzeuge

- Maßnahmen zum Schutz vor Schad-Software
- Systeme zur Einbruchserkennung (IDS/IPS)
- Festplattenverschlüsselung
- Einsatz eines VPNs zur Administration

Dies macht es Angreifern deutlich schwerer, Zugriff auf die Daten des Servers zu erlangen.

Neben dem Zugriff im laufenden Betrieb sollte auch beim Wechsel von Datenträgern darauf geachtet werden, dass die darauf befindlichen Daten sicher gelöscht werden.

### Sichere Passwörter

Nutzerinnen werden meist mittels deren Nutzernamen sowie dem zugehörigen Passwort authentifiziert. Dies betrifft sowohl das Betriebssystem wie auch den Zugang zu Mastodon. Gegebenenfalls werden Passwörter zum Boot des Systems, zur Entschlüsselung der Festplatte sowie an weiteren Stellen benötigt.

Die Firma Hive Systems, LLC diskutiert in einem aktuellen Blogbeitrag Komplexitätsanforderungen.[2] Sie geht davon aus, dass ein mindestens zwölfstelliges Passwort, welches Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthält, erst nach mehr als 200 Jahren „errechnet“ werden kann. Unter Verwendung der Hardware, die für das Training von ChatGPT verwendet wurde, sinkt der Zeitraum auf unter ein Jahr. In der Konsequenz müsste hier zu einem komplexen Passwort mit mehr als 12 Stellen geraten werden.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) geht hingegen von mindestens 8 Stellen aus[3], rät allerdings zu längeren, komplexen Passwörtern.

Die Komplexitätsanforderungen an Passwörter stellen regelmäßig ein Problem dar. Denn diese lassen sich dann nicht oder nur sehr schlecht merken. Andererseits fällt es Menschen auch meist schwer, ein komplexes, schwer zu erratendes Passwort zu erzeugen.[4] Daher ist es ratsam, auf Software zur Hilfe bei all diesen Aufgaben zurückzugreifen.

Die so genannten Passwortmanager helfen, Passwörter sicher aufzubewahren, erzeugen selbst sichere Passwörter und leisten generell einen hohen Beitrag zur Stärkung der Informationssicherheit.

Als einfache und unter verschiedenen Betriebssystemen verfügbare Software kann hier KeePassXC[5] genannt werden. Sollen Passwörter innerhalb von Teams geteilt und verwaltet werden, wäre Bitwarden einen Blick wert.[6]

### Mehrfaktorauthentisierung

Bei der Verwendung von Passwörtern wird auf das Wissen um ein Geheimnis (Passwort) als einzelner Faktor zurückgegriffen. Viele Systeme ermöglichen es, einen zweiten Faktor (beispielsweise den Besitz eines Gegenstands) mit zu verwenden.

So könnte mit einer solchen speziellen Hardware die Festplatte aufgeschlossen werden, sich Benutzerinnen am Betriebssystem oder bei Mastodon anmelden. Ohne diesen zweiten, zusätzlichen Faktor können sich Angreiferinnen nicht am System anmelden.

Als spezielle Hardware werden sehr häufig Yubikeys, Nitrokeys oder Smartcards verschiedener Hersteller verwendet. Für das Login bei Mastodon funktionieren auch Apps wie der Aegis Authenticator,[7] FreeOTP+[8] oder andere. Diese können über die App-Stores installiert werden.

## 3.3 Sichere Weitergabe der Daten

Im laufenden Betrieb kann es manchmal notwendig sein, Daten an einen anderen Speicher- bzw. Verarbeitungsort zu bewegen. Ein Umzug des Dienstes zu einem anderen Server oder nur der Umzug der Datenbank wären mögliche Szenarien. Erfahrungsgemäß ist dies oft fehlerträchtig.

Daher sollte zu Beginn gut überlegt werden, wo die Daten in welcher Form abgelegt und übertragen werden. Sofern diese auf öffentlich verfügbaren Servern liegen (Web-, FTP- oder ähnliche Server), müssen insbesondere personenbezogene Daten wirksam verschlüsselt sein. Weiterhin ist es empfehlenswert, wenn es für diese Daten eine automatische Löschroutine gibt. Damit liegen diese nicht länger als notwendig auf den Speicherorten.

2 https://www.hivesystems.io/blog/are-your-passwords-in-the-green
3 https://www.bsi.bund.de/dok/6596574, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Checklisten/sichere_passwoerter_faktenblatt.html
4 Der Sicherheitsforscher Troy Hunt pflegt eine Datenbank von Passwörtern, die durch Hacks veröffentlicht wurden. Unter https://haveibeenpwned.com/Passwords kann man in der Datenbank suchen. Selbst Begriffe wie „Grundschutz“, „ISO27001“ werden dort als von anderen verwendete Passwörter gefunden.
5 https://keepassxc.org/
6 https://bitwarden.com/
7 https://getaegis.app/
8 https://github.com/helloworld1/FreeOTPPlus

Die Übertragung der Daten muss entweder über verschlüsselte Leitungen oder verschlüsselte Datenträger erfolgen. Damit erhalten Unbefugte keinen Zugriff auf die übertragenen Daten.

### 3.4 Gewährleistung der Verfügbarkeit

Benutzerinnen spüren am ehesten Schwankungen bei der Verfügbarkeit des Dienstes. Üblicherweise möchten diese gern den Dienst nutzen, um Beiträge zu lesen oder zu verfassen und gehen davon aus, dass dieser immer ansprechbar ist. Daher ist es für die Betreiberinnen wichtig, sich Gedanken darüber zu machen.

Sofern der Server in einem Rechenzentrum betrieben wird, wird der Provider viele der Maßnahmen selbst bereitstellen. Das heißt, die Server in Rechenzentren verfügen über eine unterbrechungsfreie Stromversorgung (USV). Diese springt beim Stromausfall an und sorgt für eine gewisse Zeit für den weiteren Betrieb der Server. Weiterhin werden dort Maßnahmen zum Brandschutz sowie zur Klimatisierung der Räume getroffen.

Das heißt, auch unter diesen Aspekten ist es empfehlenswert, einen Provider zum Betrieb des Servers heranzuziehen. Sollte der Server hingegen in einer privaten Umgebung betrieben werden, so müssen sich die Betreiberinnen Gedanken zu Gegenmaßnahmen bei einem Server-Ausfall selbst machen und diese implementieren.

Eine weitere mögliche Einschränkung der Verfügbarkeit kann aus dem Ausfall von Hardware-Komponenten, insbesondere der Speichermedien, resultieren. Ein Konzept zur regelmäßigen Sicherung (Backup) und Wiederherstellung (Restore) ist daher unbedingt notwendig. Manche Provider bieten hier Lösungen an.

Häufig müssen die administrierenden Personen selbst Hand anlegen. Das bedeutet, es wird BorgBackup, restic, rsync oder ähnliche Software eingesetzt. Diese kann als Cronjob oder Systemd-Timer regelmäßig automatisch die Backup-Aufgaben ausführen und ist in der Lage, auf verschiedene Speichermedien (USB-Sticks, -Festplatten, Cloud-Speicher etc.) zu schreiben. Die Software ist in der Lage, Backups über mehrere Tage oder Wochen mitzuführen, speichert in der Regel nur Änderungen und spart dadurch Speicherplatz. Die Wiederherstellung ist auch einfach durchzuführen. Im Allgemeinen ist es sehr empfehlenswert, regelmäßig die Wiederherstellung zu testen. So bleibt man in Übung für den Notfall, und kann eventuell schneller Schreibfehler oder ähnliche Probleme feststellen.

Für Backups empfiehlt sich, die 3-2-1-Regel zu befolgen. Das bedeutet:

- **3 Kopien der Daten:** Es sollte immer mindestens drei Kopien der Datenbestände geben. Dies soll dafür sorgen, dass die Ausfallwahrscheinlichkeit minimiert wird. Denn wenn Daten nur auf einem System gespeichert sind, gibt es eine recht hohe Wahrscheinlichkeit, dass im Falle einer Wiederherstellung auch die gespeicherten Daten nicht verfügbar sind. Wenn diese jedoch auf drei unterschiedlichen und voneinander unabhängigen Systemen gespeichert sind, so ist ein Ausfall nahezu unmöglich.
- **2 verschiedene Speichermedien:** Die Kopien sollen auf mindestens zwei verschiedenen Speichermedien aufbewahrt werden.
  Die Anfälligkeit für Fehler ist bei unterschiedlichen Medien nicht gleich. Im Gegensatz kommt es des öfteren vor, dass beispielsweise Festplatten eines Herstellers aus der gleichen Serie nach etwa gleich langer Benutzungsdauer ausfallen. Die Nutzung verschiedener Hersteller und Speichermedien verlagert dies auf unterschiedliche Zeitpunkte und reduziert so die Anfälligkeit für Fehler.
- **1 Kopie an einem anderen Ort:** Mindestens eine Kopie der Daten soll sich an einem anderen Ort als die beiden anderen Kopien befinden. Im Falle eines Brandes oder eines anderen Notfalls ist so sichergestellt, dass eine Kopie immer noch verfügbar ist und benutzt werden kann.

### 3.5 Vorkehrungen für Sicherheitsvorfälle

Im Bereich der Informationssicherheit gibt es viele Expertinnen, die der Meinung sind, dass in alle Dienste eingebrochen werden wird. Es ist nur eine Frage des Zeitpunkts. Gerade auch vor diesem Hintergedanken ist es sinnvoll, Vorkehrungen für den Sicherheitsvorfall zu treffen.

Dabei kann ein Sicherheitsvorfall das Ausnutzen einer Sicherheitslücke mit anschließendem Einbruch in den Server, eine falsche Konfiguration, durch die Daten veröffentlicht werden, das Speichern einer Kopie der Datenbank im öffentlich verfügbaren Verzeichnis eines Webservers und vieles mehr sein. In der Mehrzahl der Fälle ist ein Sicherheitsvorfall

vermutlich auch eine Verletzung des Schutzes personenbezogener Daten im Sinne des Art. 4 Nr. 12 DSGVO. Daher werden diese unten gedanklich gleich behandelt.

Zunächst ist es sinnvoll, sich Gedanken zu möglichen Sicherheitsvorfällen zu machen und zu überlegen, was bei konkreten Fällen getan werden könnte. Diese Schritte können und sollen dann auch geübt werden. Dies hilft, mögliche Lücken aufzudecken und Übung für das reale Auftreten eines Vorfalls zu haben.

Neben der Beseitigung des durch einen Sicherheitsvorfall angerichteten Schadens sind insbesondere Meldepflichten im Blick zu behalten. Die DSGVO fordert im Artikel 33 eine Meldung an die Aufsichtsbehörden. Diese Meldung muss innerhalb von 72 Stunden nach Entdecken des Vorfalls geschehen. Nur für den Fall, dass der Sicherheitsvorfall zu keinen Risiken für Rechte und Freiheiten der betroffenen Personen führt, ist es zulässig, auf diese Meldung zu verzichten. Weiterhin ist bei einem voraussichtlich hohen Risiko für Rechte und Freiheiten der betroffenen Personen nach dem Art. 34 DSGVO auch eine Meldung direkt an diese Personen zu machen.

Somit müssen Informationen über Sicherheitsvorfälle schnell zu den verantwortlichen Personen gelangen. Der genaue Personenkreis hängt von der Organisationsstruktur ab. In Frage kommen hier die Geschäftsführung, Personen oder Abteilungen, die die Server administrieren oder die Informationssicherheits- bzw. Datenschutzbeauftragte. Diese sind in der Lage, sich über die Schwere des Vorfalls zu informieren und eine Entscheidung für die weitere Verfahrensweise zu treffen.

Eine Meldung muss dabei folgende Informationen enthalten:

- eine Beschreibung des Vorfalls mit Angabe der Kategorien und ungefähren Anzahl der betroffenen Personen
- Name und Kontaktdaten des Datenschutzbeauftragten oder einer anderen Anlaufstelle
- eine Beschreibung der Folgen des Vorfalls
- eine Beschreibung der getroffenen Maßnahmen zur Behebung

Die DSGVO lässt auch zu, dass die obigen Informationen schrittweise an die Aufsichtsbehörden übermittelt werden.

Am Ende eines Sicherheitsvorfalls ist es sinnvoll, den Vorfall in Ruhe zu analysieren. Dies hilft, mögliche Verbesserungen für die Zukunft zu finden und zu implementieren.

## 4. Konfiguration für den Betrieb der Software

In den unten stehenden Abschnitten werden verschiedene Software-Bestandteile und deren mögliche Konfiguration diskutiert. Dabei wird insbesondere auf eine datenschutzgerechte Einstellung Wert gelegt. Das heißt, einerseits soll die Software mit möglichst sicheren Einstellungen betrieben werden und andererseits sollen personenbezogene Daten nach Möglichkeit nicht oder nur so lange wie notwendig verarbeitet werden.

### 4.1 Einstellungen für das Betriebssystem

Das Betriebssystem, welches den Mastodon-Server wie auch die weiteren Komponenten beherbergt, sollte möglichst sicher im Sinne der Informationssicherheit sein. Das heißt, die Ziele Vertraulichkeit, Integrität und Verfügbarkeit sollten möglichst gut umgesetzt sein. Möglichst gut ist dabei im Sinne des Art. 32 Abs. 1 DSGVO zu verstehen. Das heißt, es müssen verschiedene Faktoren, wie Stand der Technik, Kosten der Umsetzung, Eintrittswahrscheinlichkeit sowie weitere, berücksichtigt werden.

#### Updates für die installierte Software

Software wird in aller Regel mit Fehlern (Bugs) ausgeliefert. In der Regel sind diese zum Zeitpunkt der Auslieferung nicht bekannt, sondern werden erst im Laufe der Zeit bekannt. Viele Herstellerinnen beheben diese Fehler und stellen Updates zur Verfügung. Einige der Fehler haben Auswirkung auf die IT-Sicherheit des zugrunde liegenden Systems. Daher ist es sinnvoll und wichtig, die Updates rechtzeitig einzuspielen. Dies kann manuell über die üblichen Administrationswerkzeuge passieren. Alternativ gibt es Werkzeuge, die den Prozess für die Aktualisierung des Systems automatisieren (Debian: unattended-upgrades). Regelmäßige Updates aller installierter Software bieten Schutz gegen bekannte Sicherheitslücken.

### Rechte für das temporäre Verzeichnis

Unter Linux werden temporäre Dateien oft in das Verzeichnis `/tmp` gespeichert. Dies kann auch ein Einfallstor für Angreiferinnen sein. Sie legen dort ausführbare Dateien ab und starten sie aus diesem Verzeichnis.

Mit dem Gedankengang sollte das Verzeichnis eine separate Partition auf dem System sein. Dies erlaubt es, das Verzeichnis mit der Option `noexec` einzubinden. Dies kann ebenfalls erreicht werden, wenn das Dateisystem tmpfs verwendet wird. Für den letzteren Fall könnte die Datei `/etc/fstab` folgende Zeile enthalten:

```
tmpfs /tmp tmpfs defaults,rw,nosuid,nodev,
noexec,relatime,size=1G  0  0
```

Damit wird ein Verzeichnis mit einer Größe von einem Gigabyte angelegt. Weiterhin sollte auf Systemen, die systemd einsetzen, die Einheit `tmp.mount` aktiv sein. Dies lässt sich mittels des Befehls `systemctl is-enabled tmp.mount` prüfen und ggf. mittels `systemctl unmask tmp.mount` aktivieren.

### Korrekte Zeit einstellen

Das Betriebssystem sowie die Anwendungen benötigen für verschiedene Aufgaben die korrekte Uhrzeit. Sofern die Systeme keinen Zugang zu anderen Mitteln haben, ist es sowohl für virtualisierte Umgebungen wie auch für physische Server sinnvoll, die Zeit mit einer oder mehreren offiziellen Quellen abzugleichen.

Hierzu eignen sich folgende Programme

- ntp
- chrony
- systemd-timesyncd

Alle gleichen die lokale Zeit mit einem Zeitserver im Internet ab. Damit ist sichergestellt, dass die korrekte Zeit eingestellt ist. Der Server sollte dabei jeweils auf genau eine Software vertrauen. Der Einsatz mehrerer verschiedener Software zur Steuerung der Systemzeit kann zu Problemen führen.

### Festplattenverschlüsselung

Neben den obigen Maßnahmen gehört auch eine Verschlüsselung der Festplatte zu den sinnvollen Maßnahmen. Üblicherweise wird die Verschlüsselung durch Eingabe eines Passworts oder durch die Anwesenheit eines Hardware-Bauteils geöffnet. Bei einem Server, der nur von der Ferne administriert wird, sind hier einige Vorkehrungen zu treffen.

Üblicherweise wird dazu die Software Dropbear installiert. Dies ist ein kleiner SSH-Server. Damit ist eine Verbindung zum Server möglich und die Festplatte kann damit aufgeschlossen werden. Genauere Anleitungen hierzu finden sich im Wiki der Thomas-Krenn AG.[9]

### Weitere Maßnahmen

Neben den oben vorgestellten Maßnahmen erscheint die Verwendung von AppArmor sinnvoll. Diese Software regelt die Zugriffsrechte von anderen Programmen über festgelegte Regeln. Einige Betriebssysteme liefern recht umfangreiche Regelsätze mit. Für Mastodon müssen jedoch selbst Regeln angelegt werden.

Weiterhin bietet Systemd eine Art Sandboxing an. Das heißt, der Dienst kann andere Systemdienste in eigenen Umgebungen „einsperren“ und nur bestimmte Zugriffe zulassen. Mittels des Befehls `systemd-analyze security servicename` werden die aktuellen Einstellungen angezeigt.
Davon ausgehend lassen sich diese mittels `systemctl edit servicename` bearbeiten. Es wäre wünschenswert, wenn seitens der Entwicklerinnen eine gehärtete Systemd-Einheit ausgeliefert wird oder sich künftig ein Projekt findet, was dies entwickelt und pflegt.

Neben den oben vorgestellten Maßnahmen lassen sich noch eine Reihe weiterer Maßnahmen zur Absicherung denken. Das Center for Internet Security bietet mit den CIS Benchmarks eine gute Quelle für weitere Maßnahmen an. Es ist empfehlenswert, diese herunterzuladen und den Hinweisen für das eigene System zu folgen.

Weiterhin bietet auch das BSI mit dem IT-Grundschutz-Kompendium eine Reihe von Bausteinen, die für die Absicherung des Systems verwendet werden können.

9 https://www.thomas-krenn.com/de/wiki/Voll-verschl%C3%BCsseltes-System_via_SSH_freischalten

### 4.2 Einstellungen für den Webserver

Als Webserver kommt nginx zum Einsatz. Dieser sollte am besten über die Paketverwaltung des jeweiligen Betriebssystems installiert werden. Dadurch wird sichergestellt, dass Aktualisierungen halb- oder ganz automatisch ankommen. In der Regel wird die Software auch so voreingestellt, dass diese als nicht-privilegierter Systembenutzer ausgeführt wird. Das reduziert die Angriffsmöglichkeiten, da dieser Systembenutzer nicht vollen Zugriff auf alle Systemdateien hat. Für den Fall einer manuellen Installation ist darauf zu achten, dass auch ähnliche Einstellungen getroffen werden.

Die Mastodon-Software bringt bei der Installation bereits eine Konfigurationsdatei für den Webserver mit.[10] Standardmäßig muss darin nur der Domain-Name ergänzt werden.

#### Versionsnummer eventuell deaktivieren

Hin und wieder wird empfohlen, die öffentlich sichtbaren Versionsnummern abzuschalten. Dazu muss in den Einstellungen, die sich üblicherweise im Verzeichnis `/etc/nginx` befinden, die Direktive `server_tokens` auf `Off` gestellt werden. Dies bietet meist nur einen geringen Schutz. Denn die von außen abfragbaren Eigenschaften des Webservers lassen sehr oft einen Schluss auf die Versionsnummer oder eine gewisse Spanne an Versionen zu.

#### TLS aktivieren

In der mitgelieferten Konfigurationsdatei sind Einstellungen für den Einsatz von TLS getroffen. Die Hauptaufgabe der Administratorinnen ist es, ein Zertifikat zu beziehen und den Speicherort der Dateien in der Konfiguration zu setzen.

Unten wird auf den Bezug eines Zertifikats mittels Let's Encrypt eingegangen. Dies ist ein recht einfacher Weg, ein Zertifikat zu beziehen. Allerdings existieren auch andere Certificate Authoritys (CA), die TLS-Zertifikate bereitstellen. Allen ist gemein, dass am Ende des Prozesses eine Zertifikats- und Schlüsseldatei steht. Der Speicherort dieser Dateien muss im Webserver eingetragen werden. Hierzu gibt es in den mitgelieferten Einstellungen für den Webserver ( `nginx.conf` ) die Zeilen `ssl_certificate` und `ssl_certificate_key` .

Dort muss der komplette Pfad zu der entsprechenden Datei eingetragen werden. Es sollte darauf geachtet werden, dass die Schlüsseldatei nur für den root-Benutzer les- und schreibbar ist.

Let's Encrypt ist eine CA, die den Bezug eines Zertifikats vereinfacht. Die Programme Certbot oder dehydrated.io sorgen dafür, dass der Aktualisierungsstand des Zertifikats geprüft und eventuell automatisch ein neues bezogen wird. Beide sollten automatisiert als Cronjob oder Systemd-Timer gestartet werden.

Im Allgemeinen sollte darauf geachtet werden, dass der Webserver nur die TLS-Versionen 1.2 oder neuer mit starken kryptografischen Algorithmen[11] verwendet. Derzeit sind alle Algorithmen, die in der Version 1.3 von TLS eingesetzt werden, als sicher anzusehen. Daneben sollten Algorithmen gewählt werden, die Authenticated Encryption (AEAD)[12] oder Perfect Forward Secrecy (PFS)[13] einsetzen. Insgesamt verbleiben damit folgende Kombinationen für TLS:[14]

```
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
```

10 siehe hierzu https://docs.joinmastodon.org/admin/install/#setting-up-nginx

11 Eine Referenz ist die Technische Richtlinie TR-02102-1 des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

12 Verschlüsselungsmodi, die GCM oder CCM einsetzen.

13 Das sind folgende Kombinationen: ECDHE_RSA, ECDHE_ECDSA, DHE_RSA, DHE_DSS

14 Siehe https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices

Je nach Sicherheitserfordernis kann die obige Auflistung weiter eingegrenzt werden. Keinesfalls sollten folgende Varianten eingestellt werden:

- NULL (keine Verschlüsselung)
- Anonymes Diffie-Hellman (aDH, keine Authentifikation)
- symmetrische Algorithmen mit einer Schlüssellänge von weniger als 128 Bit
- RC4, DES, 3DES sowie andere Algorithmen mit einer Blockgröße von 64 Bit

Diese Einstellungen liefert die Konfigurationsdatei bereits mit aus. Damit müssen keine zusätzlichen Einstellungen in dieser Hinsicht vorgenommen werden.

Weiterhin ist es sinnvoll, den Webserver so einzustellen, dass alle Anfragen zur HTTPS-Version der Seite umgeleitet werden. In der Server-Konfiguration des nginx wird dabei in zwei Teilen gearbeitet. Einer behandelt die Anfragen, die bei Port 80 ankommen und in der Regel HTTP-Anfragen ohne TLS sind. Der zweite Teil behandelt die TLS-Konfiguration. Im ersten Teil wird die folgende Zeile mit eingebaut:

```
location / { return 301 https://$host$request_uri; }
```

Dies leitet alle Anfragen auf die HTTPS-Version der Seite um.

Das Endgerät der Anwenderinnen sollte schließlich eine Information über die Verfügbarkeit von TLS erhalten. Hierzu dient die HTTP Strict Transport Security. Die Standardkonfiguration von Mastodon informiert die Endgeräte darüber, dass sie die folgenden zwei Jahre nach dem letzten Abruf die Seite über TLS erreicht werden kann.

### Logging deaktivieren

Webserver führen häufig Log-Dateien über Seiten-Zugriffe und Fehler. In den Dateien können u. a. IP-Adressen und andere personenbezogene Daten gespeichert werden. Daher ist es sinnvoll, dieses Logging entweder komplett zu deaktivieren und nur bei Bedarf (Fehleranalyse) zu aktivieren oder die Log-Dateien schnellstmöglich zu löschen.
Eine weitere Möglichkeit wäre, die IP-Adressen in den Log-Dateien ganz oder teilweise durch Nullen zu ersetzen.

Die Deaktivierung des Loggings im nginx erfolgt mittels

```
access_log off;
error_log /dev/null crit;
```

in der HTTP-Konfiguration.

Bei neueren Versionen von nginx kann auch `error_log off;` verwendet werden. Alternativ entfernen manche Betreiberinnen die IP-Adresse schon beim Schreiben in die Log-Datei. Die korrekte Konfiguration ist etwas komplexer. Es sei hierzu auf den Beitrag bei der Seite Stackoverflow verwiesen.[15] Dort wird die Konfiguration beschrieben und kann ggf. in die eigenen Einstellungen übernommen werden. Dabei sollte darauf geachtet werden, dass die Log-Datei, die Fehler aufzeichnet (error_log), entsprechend konfiguriert wird.

Sofern Log-Dateien mit personenbezogenen Daten geführt werden, sollten diese Dateien regelmäßig gelöscht werden. Die Software logrotate[16] ist hierzu hilfreich. Sie kann Log- und andere Dateien, die ein bestimmtes Alter oder eine bestimmte Dateigröße überschritten haben, löschen. Das Löschen reicht vom einfachen Entfernen aus dem Dateisystem bis zum Überschreiben mit Nullen oder Zufallswerten.

## 4.3 Einstellungen für den Datenbankserver

Wie auch der Webserver sollte die Datenbanksoftware über die Paketverwaltung des Betriebssystems installiert werden. Dadurch kommen aktuelle Versionen auf das System, und die Zugriffsrechte sind in der Regel sinnvoll gesetzt.

Die Administration und Pflege von PostgreSQL erfolgt über den Systembenutzer `postgres`. Alle diejenigen, die Administrationsaufgaben erledigen, sollten das Recht besitzen, als `postgres` zu agieren. Oft wird dies über das Programm `sudo` geregelt. Dabei ist es sinnvoll, alle Administratorinnen in einer Gruppe zur Datenbankadministration zu halten. Wenn diese Gruppe beispielsweise `dba` heißt, kann in der Datei `/etc/sudoers.d/postgres` folgendes eingestellt werden:

```
%dba ALL=(postgres) PASSWD: ALL
```

Gegebenenfalls lassen sich die Einstellungen nach Bedarf weiter verfeinern.

15 https://stackoverflow.com/a/27749834/391761
16 https://github.com/logrotate/logrotate

Der Systembenutzer `postgres` hat weitreichende Berechtigungen und kann Datenbanken wie Benutzerinnen neu anlegen, ändern etc. Im Sinne des Prinzips der geringsten Berechtigungen ist es sinnvoll, für Abfragen einer speziellen Datenbank Nutzer anzulegen, die genau dies können.

Daher sollte hierfür ein weiterer Datenbanknutzer angelegt werden. Die Mastodon-Software geht davon aus, dass dieser den Namen `mastodon` trägt. Dieser hat standardmäßig keine erweiterten Rechte. Es ist sinnvoll, dies zu kontrollieren. Als Systembenutzer `postgres` kann folgender Befehl verwendet werden:

```
psql -c "\du mastodon"
```

In der Ausgabe sollte der Benutzer nur das Attribut `Create DB` besitzen.

### 4.4 Einstellungen für Mastodon

Die Einstellungen für Mastodon selbst werden in Form von Umgebungsvariablen in einer Datei gespeichert. Diese Datei liegt in dem Verzeichnis, in dem die Mastodon-Software installiert wurde und heißt standardmäßig `.env.production`

#### Keine IP-Adressen speichern

Mastodon speichert den Zeitpunkt des letzten Logins mit der jeweiligen IP-Adresse in der Datenbank. Dies erscheint zumeist nicht notwendig. Daher ist es sinnvoll, dies zu deaktivieren. In der oben erwähnten Konfigurationsdatei `.env.production` sollte daher die Variable `IP_RETENTION_PERIOD` auf `0` gesetzt werden.

#### Secure Mode aktivieren

Eine Besonderheit bei Mastodon ist der so genannte „Secure Mode“. Server, die in dem Modus betrieben werden, erfordern es, dass alle Anfragen signiert werden. Dadurch lässt sich steuern, inwieweit öffentliche Nachrichten auf blockierten Servern zu sehen sind. Mit aktiviertem Secure Mode werden diese Inhalte dort nicht angezeigt.

Allerdings bleiben die Inhalte weiterhin über die Webseite verfügbar. Über andere Instanzen können diese eventuell ebenfalls abgerufen werden. Insofern ist das nur ein recht schwacher Schutz für öffentliche Inhalte. Nicht-öffentliche Inhalte erfordern hingegen immer eine Authentifizierung.

Bei Mastodon werden HTTP-Anfragen genutzt, um Informationen abzurufen. Das heißt, ein Client nutzt eine definierte Schnittstelle (Application Programming Interface, API) und sendet meist mittels der GET-Methode Anfragen ab. Ohne aktivierten Secure Mode können so Toots, Profilinformationen und anderes abgerufen werden.

Wenn ein Server den Secure Mode aktiviert hat, können diese Informationen nur mit Hilfe einer Signatur abgerufen werden. Diese Signatur wird vom Server nur bei einer eingeloggten Benutzerin erzeugt. Mit der signierten Anfrage kann der andere Server entscheiden, ob die gewünschten Informationen übermittelt werden oder nicht. Letzteres kann der Fall sein, wenn der Account blockiert ist.

Das Erstellen und Prüfen der Signaturen ist in der Regel rechenaufwendig. Daher ist dies nicht standardmäßig aktiv. Wenn dies aktiviert werden soll, muss in der `.env.production` der Wert von `AUTHORIZED_FETCH` auf `1` gestellt werden.

Neben der möglichen höheren Rechenleistung kann es auch sein, dass andere Instanzen im Fediverse Probleme mit dem Secure Mode haben. So musste bei der Diskussionsplattform Lemmy bei Versionen vor der 0.19.4 eine Einstellung aktiviert werden. Falls dem nicht so war, konnten diese Instanzen nicht mit Mastodon-Instanzen mit aktiviertem Secure Mode kommunizieren. Ähnliches ist auch bei anderer Fediverse-Software denkbar, wenn auch derzeit nicht öffentlich bekannt.

Andererseits gibt es auch Software, wie beispielsweise GoToSocial, die Secure Mode standardmäßig aktiviert haben.

Bei der Entscheidung für oder gegen den Secure Mode sollte auch der Umgang mit der Plattform Threads in Erwägung gezogen werden. Im Fediverse gibt es viele Menschen, die aus unterschiedlichen Überlegungen die Plattform von Meta blockieren möchten. Sollte sich die Betreiberin hierfür entscheiden, so würde der Secure Mode dies effektiver machen.

Insgesamt sollten Betreiberinnen daher abwägen, ob sie den Secure Mode aktivieren möchten. Es fällt schwer, hier einen allgemein gültigen Rat zu geben.

# Verzeichnis von Verarbeitungstätigkeiten und Schwellwertanalyse

## Vorausgefüllte Muster und Dokumentation der technischen und organisatorischen Maßnahmen

Zu den Pflichten der DSGVO gehört es, ein Verzeichnis von Verarbeitungstätigkeiten zu führen. Beim Betrieb eines Mastodon-Servers sollte hierbei zwischen angemeldeten Nutzerinnen und Gastzugriffen über die öffentlich verfügbare Website unterschieden werden. Für beide Verarbeitungstätigkeiten stehen beispielhafte Einträge als Muster zur Verfügung.

**MUSTER FÜR EIN VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN**

https://sds-links.de/mastodon-muster-vvt

Angaben zur Verantwortlichen:
Angaben zur Vertreterin der Verantwortlichen:
Angaben zur Datenschutzbeauftragten:

Verarbeitungstätigkeiten
Zweck der Verarbeitung:
Bereitstellung einer Plattform zur öffentlichen Kommunikation

Beschreibung des Verfahrens:
Der Betrieb eines Mastodon-Servers soll es verschiedenen Stellen ermöglichen, Kurznachrichten öffentlich zu tauschen und in Kommunikation mit anderen zu treten.

→ vollständiges Muster auf der Webseite

Zu einem Verzeichnis der Verarbeitungstätigkeiten gehört es ebenfalls, die technischen und organisatorischen Maßnahmen (TOMs) zu dokumentieren. Diese unterscheiden sich stark, je nachdem ob ein Server in eigenen Räumlichkeiten oder als gemieteter Server in einem Rechenzentrum betrieben wird. Für beide Fälle steht eine beispielhafte Dokumentation zum Download bereit.

**DOKUMENTATION VON TOMS BEIM BETRIEB EINES SERVERS IN EIGENEN RÄUMLICHKEITEN**

https://sds-links.de/mastodon-muster-toms-on-prem

Vertraulichkeit
Zutrittskontrolle:
Maßnahmen, die Unbefugten den Zutritt zu IT-Systemen, die personenbezogene Daten verarbeiten, verwehren sollen.

→ vollständiges Muster auf der Webseite

**DOKUMENTATION VON TOMS BEIM BETRIEB EINES IN EINEM RECHENZENTRUM GEMIETETEN SERVERS**

https://sds-links.de/mastodon-muster-toms-rz

Diese unten beschriebenen technischen und organisatorischen Maßnahmen gehen davon aus, dass ein Server (virtueller Server, Root-Server oder ähnliches) bei einem Provider in einem Rechenzentren gemietet wurde. Die Aufgabe des Providers ist es unter anderem, verschiedene technische und organisatorische Maßnahmen zur Absicherung des Servers sicherzustellen. Diese werden üblicherweise im Vertrag zur Auftragsverarbeitung bzw. den Anhängen zum Vertrag genauer beschrieben.

→ vollständiges Muster auf der Webseite

Des weiteren sollte eine Schwellwertanalyse zur Feststellung des mit dem Betrieb der Instanz verbundenen Risikos durchgeführt werden. Wenn eine Verarbeitung voraussichtlich hohe Risiken für Rechte und Freiheiten hat, muss eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt werden. Eine Schwellwertanalyse hilft bei der Einschätzung, ob derartige hohe Risiken gegeben sind. Das bereitgestellte Muster soll dabei unterstützen, eine Schwellwertanalyse korrekt und systematisch durchzuführen.

**MUSTER FÜR EINE SCHWELLWERTANALYSE ZUM BETRIEB EINES MASTODON-SERVERS**

https://sds-links.de/mastodon-muster-schwellwertanalyse

Allgemeine Angaben
Anforderungen aus Art. 35 DSGVO
Muss-Liste der Aufsichtsbehörden
Kriterien aus dem Working Paper 248
Ergebnis der Prüfung

→ vollständiges Muster auf der Webseite

# Informationen für eine Auskunft nach Art. 15 DSVGO

Dieses Kapitel erklärt, wie Informationen für eine Auskunft nach Art. 15 DSGVO einer betroffenen Person recherchiert werden können. Die unten angesprochenen Informationen finden sich in der Datenbank des Mastodon-Servers.

Wenn die Installation nach der Anleitung auf der Mastodon-Webseite vorgenommen wurde, heißt die Datenbank `mastodon_production`. Gegebenenfalls muss der korrekte Name der Datenbank ausgewählt werden.

Es wird angenommen, dass die betreffende Person sich entweder über deren Mastodon-Namen oder über eine E-Mail-Adresse meldet und anhand dieser Daten Auskunft begehrt.

## Ermittlung von account_id und user_id

Die entsprechenden personenbezogenen Daten befinden sich in der Datenbank und werden dort über den Wert `account_id` oder `user_id` referenziert. Die `account_id` ist eine interne Nummer des Mastodon-Namens. Die `user_id` ist eine Nummer, die von der Software für die Benutzerinnen vergeben wird.

## Unter Benutzung der E-Mail-Adresse

Sollten die Nutzerinnen Auskunft anhand der E-Mail-Adresse begehren, so können beide Id-Nummern folgendermaßen ermittelt werden:

```
SELECT id AS user_id, account_id FROM users
WHERE email LIKE 'email@address';
```

Dabei muss `email@address` durch die korrekte E-Mail-Adresse ersetzt werden. Die obige Abfrage ergibt eine Tabelle mit zwei Spalten, die die entsprechenden Werte enthalten.

## Unter Benutzung des Mastodon-Namens

Falls jemand eine Auskunft mittels des Mastodon-Namens haben möchte, ist die Anfrage zweiteilig zu gestalten. Zunächst wird die `account_id` ermittelt und danach die `user_id`.

```
SELECT id FROM accounts WHERE domain is null
AND username LIKE 'username';
```

```
SELECT id AS user_id, account_id FROM users
WHERE account_id = nummer;
```

Bei den obigen Anfragen wird als `username` der Name eingesetzt, der von der betreffenden Person genannt wurde. Das Ergebnis der ersten Anfrage wird dann als `nummer` in die zweite Anfrage eingesetzt. Erfahrene Datenbank-Administratorinnen können beide Anfragen kombinieren.

Das Ergebnis der letzten Anfrage enthält die `account_id` sowie die `user_id`.

## Unter Benutzung eines Toots

Schließlich gäbe es die Möglichkeit, dass jemand unter Angabe eines Toots Auskunft begehrt. Es ist zu erwarten, dass die URL zum Toot als Referenz angegeben wird. Diese hat folgende Struktur.

https://example.org/@username/zahl bzw.
https://example.org/@username@instanzname/zahl

Anhand der Zahl, der Identifikationsnummer des Toots, lässt sich die `account_id` ermitteln:

```
SELECT account_id FROM statuses WHERE id =
zahl;
```

Alternativ lässt sich nach der URL oder Teilen davon suchen:

```
SELECT account_id FROM statuses WHERE url LIKE 'suchbegriff';
```

Mit diesen Anfragen wird die `account_id` ermittelt und kann für untenstehende Recherchen verwendet werden.

## Ermittlung der personenbezogenen Daten

Nachdem nun `account_id` und `user_id` bekannt sind, können die Angaben aus der Datenbank extrahiert werden. In der Mehrzahl der Fälle sind die Tabellen mit der `account_id` verknüpft.

Es gibt jedoch auch solche Tabellen (z. B. `backups`, `login_activities` etc.), die die `user_id` referenzieren.

Die wichtigsten Tabellen sind `accounts` und `users`. Die erstgenannte Tabelle enthält den Mastodon-Namen, den Namen und viele weitere spezifische Angaben. Die Tabelle `users` enthält insbesondere die E-Mail-Adresse und weitere Daten.

Neben den beiden oben genannten Tabellen gibt es in der Datenbank weitere Tabellen, die personenbezogene Daten enthalten können. Für eine Recherche zu personenbezogenen Daten empfiehlt es sich, diese mit der oben ermittelten `account_id` oder `user_id` abzufragen.

Mittels `\d tabellenname;` lässt sich eine Beschreibung der Tabelle mit Namen, Datentyp und weiteren Angaben zu den Tabellen anzeigen. Eine Anfrage der folgenden Art gibt alle Informationen aus einer Spalte zu einer `account_id an`. Unten wurde die Tabelle `tag_follows` (Tags, denen Benutzerinnen folgen) als Beispiel ausgewählt:

```
SELECT * FROM tag_follows WHERE account_id = 11223344;
```

```
 id | tag_id |account_id|         created_at         |         updated_at
----+--------+----------+----------------------------+----------------------------
  1 |   4358 | 11223344 | 2023-05-16 21:50:55.940761 | 2023-05-16 21:50:55.940761
(1 row)
```

# Impressum

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

STIFTUNG DATENSCHUTZ

**Autorinnen**
Jens Kubieziel, Malte Engeler, Rebecca Sieber
für die Stiftung Datenschutz

**Idee und Projektleitung**
Hendrik vom Lehn

**Redaktionelle Bearbeitung**
Theresa Wenzel

**Version**
V 1.1, Stand September 2024

**Agenturpartner**
KING CONSULT | Kommunikation

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

Bundesministerium der Justiz