

Gruppen sicher organisieren

Wer eine Gruppe, ein Forum oder eine Spielrunde betreibt, trägt Verantwortung für fremde Daten und fremde Erfahrungen. Was vorher geklärt sein sollte — und was im Konfliktfall hilft.

THEMEN IM ÜBERBLICK

Rollen & Rechte

Regeln, die tragen

Umgang mit Störern

Treffen & Termine

Voice & Bildschirm

Minderjährige

Fremde Daten

Wenn es eskaliert

Diese Broschüre richtet sich an Menschen, die etwas betreiben: Gruppenadministration, Forenmoderation, Spielrunden, Vereins- oder Nachbarschaftsgruppen. Die Sicht der Teilnehmenden behandelt „**Social Media Sicherheit**“.

01	Was Sie übernehmen, wenn Sie gründen	3
02	Rollen und Rechte	4
03	Regeln, die im Ernstfall tragen	5
04	Umgang mit Störern	6
05	Treffen, Termine und Adressen	7
06	Voice, Video und Bildschirmfreigabe	8
07	Minderjährige in der Gruppe	9
08	Fremde Daten, die Sie verwalten	10
09	Wenn es eskaliert	11
10	Spickzettel zum Ausdrucken	12
11	Quellen und weiterführende Hinweise	13
12	Impressum und Weitergabe	14



Plattformunabhängig

Ob Messenger-Gruppe, Forum, Spieleserver oder Vereinsplattform: Die Fragen sind überall dieselben, nur die Knöpfe heißen anders.

Was Sie übernehmen, wenn Sie gründen

Eine Gruppe zu eröffnen dauert zehn Sekunden. Damit übernehmen Sie aber drei Dinge, die selten mitgedacht werden: fremde Daten, fremde Erfahrungen und die Frage, wer entscheidet, wenn es Streit gibt.

Fremde Daten

Mitgliederlisten, Telefonnummern, Adressen für Treffen, Fotos. Alles davon gehört anderen Menschen, nicht Ihnen.

Fremde Erfahrungen

Wer sich in Ihrer Gruppe unwohl fühlt, geht meist stillschweigend. Sie erfahren von Problemen zuletzt — oder nie.

Entscheidungsgewalt

Sie können ausschließen, löschen und Rechte vergeben. Diese Macht ist nötig, sollte aber vorher beschrieben sein.

Nachfolge

Was passiert, wenn Sie ausfallen? Eine Gruppe mit genau einer administrierenden Person ist eine Gruppe auf Zeit.

VIER FRAGEN VOR DEM START

Wer darf hinein? Wer darf hinauswerfen? Was passiert mit den Daten, wenn jemand geht? Und wer übernimmt, wenn Sie es nicht mehr machen? Wer diese vier Fragen einmal beantwortet, spart sich die meisten späteren Konflikte.

Rollen und Rechte

Die häufigsten zwei Fehler sind Spiegelbilder voneinander: Alle bekommen alle Rechte, weil es unkompliziert ist — oder eine Person behält alles, weil sie es am besten weiß.

ROLLE	SOLLTE DÜRFEN	SOLLTE NICHT DÜRFEN
Mitglied	Lesen, schreiben, eigene Beiträge bearbeiten und löschen	Andere einladen, ohne dass es jemand mitbekommt
Moderation	Beiträge ausblenden, stummschalten, Meldungen bearbeiten	Die Gruppe auflösen oder Rollen an sich selbst vergeben
Administration	Alles, inklusive Rollenvergabe und Einstellungen	Alleiniger Zugang sein — es braucht immer eine zweite Person

- ✓ Mindestens zwei administrierende Personen, damit ein Kontoverlust die Gruppe nicht handlungsunfähig macht.
- ✓ Rechte nach Bedarf vergeben, nicht nach Verdienst. Wer nur Termine einträgt, braucht keine Rechte zum Löschen.
- ✓ Rollen regelmäßig durchsehen. Inaktive Moderation ist eine offene Tür, wenn das Konto übernommen wird.
- ✓ Alle Konten mit erweiterten Rechten sollten 2FA nutzen — siehe „Cybersecurity im Alltag“, Kapitel „2FA, Passkeys und Hardwarekeys“.

Regeln, die im Ernstfall tragen

Regeln werden fast immer erst geschrieben, wenn es das erste Mal Ärger gab — und dann wirken sie wie eine Maßnahme gegen eine bestimmte Person. Vorher aufgeschrieben sind sie neutral.

Kurz

Fünf bis sieben Punkte, die man in einer Minute liest. Alles Längere liest niemand und niemand kann sich darauf berufen.

Konkret

„Keine Beleidigungen“ ist auslegbar. „Wir duzen uns, wir greifen Argumente an, nicht Personen“ ist überprüfbar.

Mit Folgen

Was passiert beim ersten, was beim wiederholten Verstoß? Ohne Stufen bleibt nur alles oder nichts.

Sichtbar

Angepinnt, in der Beschreibung, in der Begrüßungsnachricht. Regeln, die man suchen muss, gelten nicht.

Was hineingehört

- ✓ Worum es in der Gruppe geht — und worum ausdrücklich nicht.
- ✓ Umgangston und was als Grenzüberschreitung gilt.
- ✓ Ob Screenshots und Weitergabe von Inhalten nach außen erlaubt sind.
- ✓ Wie gemeldet wird und wer entscheidet.
- ✓ Was mit Beiträgen passiert, wenn jemand die Gruppe verlässt.
- ✓ Ob Werbung, Umfragen und Weiterleitungen erwünscht sind.

Umgang mit Störern

Nicht jeder Konflikt ist Moderationssache, und nicht jede Störung ist böse gemeint. Hilfreich ist eine Reihenfolge, die man auch dann einhält, wenn man selbst gereizt ist.

1 Privat ansprechen. Viele Fälle enden hier. Öffentliche Zurechtweisung erzeugt Publikum und Fronten.

2 Öffentlich einordnen, wenn nötig — sachlich und mit Bezug auf die Regel, nicht auf die Person.

3 Vorübergehend stummschalten. Die wirksamste Stufe: Sie kühlt ab, ohne endgültig zu sein.

4 Ausschließen, wenn es sich wiederholt oder wenn die Grenzüberschreitung schwer wiegt.

5 Dokumentieren. Wer wann was — kurz und intern. Spätestens bei der Beschwerde brauchen Sie es.

! Sofort und ohne Stufen

Bei Bedrohungen, sexuellen Übergriffen, Aufnahmen ohne Einverständnis oder Kontaktversuchen zu Minderjährigen gibt es keine Verwarnung: sofort ausschließen, Beweise sichern, bei der Plattform melden und je nach Fall Anzeige erstatten.

i Der stille Abgang

Die meisten Betroffenen beschwerten sich nicht, sie verschwinden. Ein gelegentliches, ausdrückliches Angebot — „meldet euch bei mir, auch vertraulich“ — bringt Fälle ans Licht, die Sie sonst nie erfahren.

Treffen, Termine und Adressen

Sobald aus einer Online-Gruppe ein Treffen wird, entstehen die heikelsten Daten überhaupt: Wer ist wann wo — und wessen Wohnung steht offen im Chat.

Adressen nur an Zusagen

Die genaue Anschrift erst an Personen, die tatsächlich kommen — nicht in die offene Einladung.

Abwesenheit verrät

„Wir sind alle Samstag ab 18 Uhr bei Tom“ sagt auch, welche Wohnungen dann leer sind. In offenen Gruppen ein echtes Risiko.

Teilnehmerlisten

Wer kommt, ist eine personenbezogene Information. Sichtbarkeit bewusst wählen, nicht dem Standard überlassen.

Fotos vom Treffen

Vorher fragen, nicht nachher. Und akzeptieren, wenn jemand nicht möchte — auch ohne Begründung.

ÖFFENTLICHE KALENDERLINKS

Geteilte Kalender und Einladungslinks sind bequem und werden gern weitergereicht. Prüfen Sie, ob ein Link wirklich **nur** den Termin zeigt — und nicht gleich die ganze Teilnehmerliste mit Kontaktdaten. Links, die einmal öffentlich waren, lassen sich nicht zurückholen; sie müssen ersetzt werden.

Voice, Video und Bildschirmfreigabe

In Sprachrunden passiert vieles beiläufig — und genau dort entstehen die Situationen, die hinterher niemand gewollt hat.

- ✓ Zu Beginn sagen, wer alles im Raum ist. Stille Zuhörende sind der häufigste Grund für unangenehme Überraschungen.
- ✓ Aufzeichnungen nur mit Ansage und Zustimmung. Heimliche Mitschnitte sind je nach Land strafbar.
- ✓ Vor der Bildschirmfreigabe aufräumen: Nur das gewünschte Fenster teilen, nicht den ganzen Bildschirm. Benachrichtigungen vorher stummschalten.
- ✓ Mikrofon standardmäßig stumm beim Beitreten. Das schützt vor dem klassischen Nebenraumgespräch.
- ✓ Wer moderiert, sollte stummschalten und entfernen können — ohne dazu Administrationsrechte für die ganze Gruppe zu brauchen.

! Der geteilte Bildschirm

Die häufigste Datenpanne in Gruppen ist keine Attacke, sondern eine Bildschirmfreigabe: eine aufpoppende Nachricht, ein offener Passwortmanager, eine Mailübersicht. Ein eigener, aufgeräumter Nutzer oder ein zweiter Bildschirm löst das dauerhaft.

Minderjährige in der Gruppe

Sobald Jüngere dabei sind, ändern sich die Maßstäbe — unabhängig davon, ob die Gruppe für sie gedacht war. In Spiel- und Hobbygruppen ist das eher die Regel als die Ausnahme.

- ✓ Damit rechnen, dass Jüngere dabei sind, auch wenn es niemand sagt. Der Umgangston sollte das aushalten.
- ✓ Keine Direktnachrichten von Erwachsenen an Minderjährige ohne erkennbaren Anlass — das gilt auch für wohlmeinende.
- ✓ Bei Treffen: Sorgeberechtigte informieren, Ansprechperson benennen, Zeiten klar regeln.
- ✓ Kontaktversuche, die auf Geheimhaltung zielen, sofort ernst nehmen und melden.
- ✓ Bei Verdacht nicht selbst ermitteln, sondern dokumentieren und weitergeben.

i Woran man Grooming erkennt

Die typischen Muster — auffällige Zuwendung, Geschenke im Spiel, Wechsel auf einen privaten Kanal, Bitte um Geheimhaltung — stehen mit Handlungsanleitung in „Kinder online begleiten“, Kapitel „Grooming erkennen“.

Fremde Daten, die Sie verwalten

Mitgliederlisten, Kontaktdaten, Fotos, Anwesenheiten: Wer eine Gruppe organisiert, verarbeitet personenbezogene Daten anderer. Bei rein privaten Gruppen greift das Datenschutzrecht meist nicht — bei Vereinen, Kursen und allem Öffentlichen schon.

- ✓ **Sparsam erheben.** Für eine Spielrunde braucht es keine Anschrift und kein Geburtsdatum.
- ✓ **Zweckgebunden nutzen.** Kontaktdaten für die Terminabsprache sind kein Verteiler für Werbung.
- ✓ **Nicht weitergeben,** auch nicht an andere Mitglieder, ohne zu fragen.
- ✓ **Löschen, wenn jemand geht** — und vorher sagen, was mit den Beiträgen passiert.
- ✓ **Bei E-Mails an alle: BCC.** Ein offener Verteiler ist die klassische kleine Datenpanne.
- ✓ **Zugriff begrenzen.** Nicht jede moderierende Person braucht die vollständige Mitgliederliste.

i Wenn jemand Auskunft verlangt

Mitglieder dürfen erfahren, was Sie über sie gespeichert haben, und Löschung verlangen. Wie ein solcher Antrag aussieht und welche Fristen gelten, steht in „**Deine Rechte an deinen Daten**“, Kapitel „So stellen Sie einen Antrag“ — dieselben Regeln, nur aus der anderen Richtung gelesen.

REIHENFOLGE IM ERNSTFALL

Sichern – trennen – melden – informieren. Erst Beweise, dann die Person entfernen, dann die Plattform einschalten, dann die Gruppe sachlich informieren.

FALL	WAS ZU TUN IST
Belästigung, Beleidigung	Screenshots sichern, ausschließen, bei der Plattform melden, Betroffene fragen, ob sie Unterstützung möchten.
Bedrohung oder Nötigung	Beweise sichern und Anzeige erstatten. Betroffene entscheiden, ob sie selbst anzeigen – drängen Sie nicht.
Übernommenes Konto in der Gruppe	Rechte sofort entziehen, Gruppe warnen, betroffene Person über einen anderen Kanal erreichen.
Daten sind abgeflossen	Betroffene informieren, was genau betroffen ist. Bei Vereinen und öffentlichen Angeboten kann eine Meldepflicht bestehen.
Streit ohne Regelverstoß	Nicht moderieren, sondern moderieren lassen: Thema schließen, Gespräch anbieten, Abstand ermöglichen.

Beweise richtig sichern

Screenshot mit Profilname, Datum, Uhrzeit und vollständigem Inhalt, dazu die Adresse des Beitrags. Ausführlich in „**Social Media Sicherheit**“, Kapitel „Belästigung, Mobbing und richtig melden“.

Spickzettel zum Ausdrucken

BEIM GRÜNDEN GEKLÄRT

-  Wer darf hinein
-  Wer darf ausschließen
-  Was passiert mit Daten beim Austritt
-  Zweite administrierende Person

LAUFEND

-  Regeln sichtbar angepinnt
-  Rollen durchgesehen
-  2FA bei allen mit Rechten
-  Alte Einladungslinks ersetzt

BEI TREFFEN

-  Adresse nur an Zusagen
-  Teilnehmerliste nicht offen
-  Fotos vorher abgesprochen
-  Ansprechperson benannt

IM KONFLIKTFALL

-  Beweise gesichert
-  Erst privat angesprochen
-  Entscheidung dokumentiert
-  Betroffene gefragt, was sie brauchen

WENN SIE NUR EINE SACHE TUN

Schreiben Sie fünf Regeln auf und pinnen Sie sie an — **bevor** es den ersten Konflikt gibt. Danach wirkt jede Regel wie ein Urteil über eine bestimmte Person.

Quellen und weiterführende Hinweise

klicksafe: Moderation und Community-Management
klicksafe.de → Themen

jugendschutz.net: Meldestelle für Online-Inhalte
jugendschutz.net

BfDI: Betroffenenrechte der DSGVO
bfdi.bund.de → Bürgerinnen und Bürger

Verordnung (EU) 2016/679 – DSGVO im Volltext
eur-lex.europa.eu → CELEX:32016R0679

Verbraucherzentrale: Vereine und Datenschutz
verbraucherzentrale.de → Digitale Welt → Datenschutz

Polizeiliche Kriminalprävention: Anzeige erstatten
polizei-beratung.de → Themen

Nummer gegen Kummer: Beratung für Jugendliche und Eltern
nummergegenkummer.de

Datenschutzkonferenz: Kurzpapiere
datenschutzkonferenz-online.de

Hinweis

Diese Broschüre ersetzt keine Rechtsberatung. Ob und in welchem Umfang das Datenschutzrecht für Ihre Gruppe gilt, hängt davon ab, wie privat oder öffentlich sie ist. Im Zweifel bei der Aufsichtsbehörde nachfragen.

Weitere Broschüren dieser Reihe

- Cybersecurity im Alltag** — Links, Phishing, Passwörter, 2FA, DNS, öffentliche WLANs und Notfälle.
- Social Media Sicherheit** — Konten, Privatsphäre-Einstellungen, Fake-Profilе, Datenweitergabe.
- Smartphone absichern** — Sperre, Berechtigungen, App-Quellen, Verlust, Gerätewechsel, Backups.
- Heimnetz und Smart Home** — Router, WLAN, Gastnetz, vernetzte Geräte, Kameras, Portfreigaben.
- Kinder online begleiten** — Für Eltern: Altersgrenzen, Regeln, Mobbing, Grooming, Anlaufstellen.
- Deine Rechte an deinen Daten** — DSGVO praktisch: Auskunft, Löschung, Übertragbarkeit, Musterschreiben.
- Gruppen sicher organisieren** — diese Broschüre
- Allergene und Kennzeichnung** — Die 14 Pflichtangaben, Zutatenlisten lesen, „kann Spuren enthalten“.
- Erste Schritte** — Zweiseitiges Merkblatt zum Einstieg — kein Heft.

Weitergabe und Lizenz

Herausgeber

Plotspace.eu · info@plotspace.eu
Anschrift und Verantwortlicher im Impressum:
plotspace.eu/impressum

Lizenz

CC BY 4.0 — Kopieren, Weitergeben und Bearbeiten ausdrücklich erlaubt. Bitte „Plotspace.eu“ als Quelle nennen und Änderungen kenntlich machen; bearbeitete Fassungen dürfen nicht so wirken, als kämen sie von Plotspace.eu. creativecommons.org/licenses/by/4.0/deed.de
Schriften: Public Sans und IBM Plex Mono, SIL Open Font License 1.1.

Diese Broschüre darf einzeln weitergegeben werden. Sie ist so aufgebaut, dass sie für sich allein verständlich bleibt; Querverweise auf die übrigen Hefte sind Ergänzung, keine Voraussetzung.