Datenschutz in sozialen Medien

Was gilt es bei der Nutzung von sozialen Medien zur Erreichung der Zielgruppe des Förderprogramms IQ zu beachten?

Stand: September 2026

1. Hintergrund

Das Erstellen und Verbreiten von Informationen in sozialen Medien gehört inzwischen zum festen Bestandteil vieler Projekte und Vorhaben im Bereich Anerkennung und Migration. Soziale Medien werden aber auch zunehmend genutzt, um aktiv auf Zugewanderte oder auf Unternehmen zuzugehen, die Zugewanderte beschäftigen oder beschäftigen möchten – und um in digitalen Räumen die (Arbeitsmarkt-)Integration zu unterstützen. Anders als bei der Präsenzberatung und -arbeit gewinnen dabei Fragen des Datenschutzes und des Umgangs mit diesem sich durch die nationale und europäische Rechtsprechung und Gesetzgebung sowie die Internationalisierung der genutzten Tools und Plattformen immer dynamischer entwickelnden Bereichs stetig an Bedeutung. Für Vorhaben wird es immer schwieriger, sich im „Dschungel“ der Vorschriften, Verordnungen und Urteile zurechtzufinden und „datenschutzkonform“ zu verhalten.

Aus diesem Grund unterstützt die Fachstelle Einwanderung und Integration auch in der aktuellen Förderrunde 2026-2028 die IQ Vorhaben bei grundsätzlichen und aktuellen Fragen zum Umgang mit datenschutzrechtlichen Vorgaben bei der Arbeit in sozialen Medien. Dabei arbeitet die Fachstelle eng mit auf Datenschutz und die aufsuchende Arbeit in sozialen Medien spezialisierten Minor-Projekten zusammen, etwa Social Media Bridge - Aufsuchende Beratung für Geflüchtete in den sozialen Medien (SoMB) oder Social Media Streetwork - Erstinformation und Verweisberatung in sozialen Medien gegen Marginalisierung (SoMS). Ergänzt wird die Arbeitshilfe durch Auszüge aus der Publikation „Beratungsrichtlinien. Version 5.0“, die im Projekt „CADS – Community Advisors – Digital Streetwork für EU-Beschäftigte in Deutschland“ von Minor – Digital entstanden ist.

Mit dieser Arbeitshilfe erhalten die IQ Vorhaben ein Nachschlagewerk für zentrale Fragen der DSGVO-konformen Arbeit. Sie ist als *living document* angelegt und wird regelmäßig aktualisiert. Es handelt sich dabei nicht um eine Rechtsberatung und soll diese auch nicht ersetzen.

Inhaltsverzeichnis

2. Allgemeines zum Datenschutz

- **Rechtsgrundlagen:** Die zentrale Rechtsgrundlage für Datenschutz ist die Datenschutz-Grundverordnung (DSGVO). Nationale Gesetze wie das Bundesdatenschutzgesetz (BDSG) und Landesdatenschutzgesetze ergänzen die DSGVO.
- **Der zentrale Begriff in der DSGVO:** personenbezogene Daten (Definition in Art. 4 Ziff. 1 DSGVO)
- **Grundsatz: Verbot mit Erlaubnisvorbehalt (Art. 6 DSGVO):** Damit eine Datenverarbeitung rechtmäßig ist, muss mindestens eine der Rechtsgrundlagen des Art. 6 erfüllt sein.
- **Wichtig:** Es ist ratsam, rechtzeitig im eigenen Interesse ein vollständiges Verzeichnis von Verarbeitungstätigkeiten zu erstellen (Art. 30 DSGVO).

2.1 Was sind personenbezogene Daten?

- Name und Vorname
- Geburtsdatum
- Kontaktdaten (z.B. Adresse, E-Mail-Adresse, Telefonnummer etc.)
- Körperliche Merkmale (z.B. Größe, Gewicht etc.)
- Wohnverhältnisse/Vermögensverhältnisse/Bankverbindung
- Geistige Zustände (z.B. Einstellungen, Überzeugungen etc.)
- Weitere Daten (z.B. Standortdaten, Nutzungsdaten, Handlungen, Äußerungen, Werturteile, beruflicher Werdegang etc.)

2.2 Formen des Umgangs mit personenbezogenen Daten

- Erheben
- Verarbeiten
- Nutzen
- Privacy by design/privacy by default
    - » Datenschutz ist schon beim Planen neuer Techniken und Verarbeitungen sowie durch datenschutzfreundliche Grundeinstellungen zu berücksichtigen.

2.3 Grundsätze der Verarbeitung personenbezogener Daten

<u>Artikel 5 DSGVO</u>

(1) Personenbezogene Daten müssen

a) … auf rechtmäßige Weise **… („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**“),

b) … für festgelegte, eindeutige und legitime Zwecke … („**Zweckbindung**“),

c) … auf das notwendige Maß beschränkt … („**Datenminimierung**“, “**Datensparsamkeit**“),

d) … sachlich richtig … („**Richtigkeit**“),

e) … erforderlich … („**Speicherbegrenzung**“) [und mit]

f) … angemessener Sicherheit … („**Integrität und Vertraulichkeit**“)

verarbeitet werden.

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („**Rechenschaftspflicht**“).

Verbot mit Erlaubnisvorbehalt (Art. 6 DSGVO)

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

- **Einwilligung** der betroffenen Person
- Die Verarbeitung für **Erfüllung eines Vertrages** oder zur **Durchführung vorvertraglicher Maßnahmen**
- Die Verarbeitung für **Erfüllung einer rechtlichen Verpflichtung**
- Die Verarbeitung zum **Schutz der lebenswichtigen Interessen** (subsidiär)
- Die Verarbeitung im **öffentlichen Interesse** oder **in Ausübung öffentlicher Gewalt**, die dem Verantwortlichen übertragen wurde
- Die Verarbeitung zur **Wahrung der berechtigten Interessen des Verantwortlichen** sofern nicht die Interessen der betroffenen Person überwiegen (Generalklausel)

2.4 Richtiger Umgang mit Daten

Bewerten:

- Welche Daten habe ich?
- Welche Daten benötige ich?
- Wann kann ich die Daten entsorgen?

Falls die Datenerfassung zu Dokumentationszwecken notwendig ist, sollten die Erhebung, Nutzung und Verarbeitung der Daten anonym erfolgen.

3. Datenschutz in sozialen Medien

Die Dienste von Meta (Facebook und Instagram), YouTube/Google und LinkedIn werden für Nutzende in der EU jeweils von Tochtergesellschaften mit Sitz in Irland erbracht; die Konzernmütter sitzen in den USA. Bei TikTok sind für den EWR TikTok Technology Limited (Irland) und TikTok Information Technologies UK Limited verantwortlich; Mutterkonzern ist das chinesische Unternehmen ByteDance. Alle diese Unternehmen übermitteln regelmäßig personenbezogene Daten aus der Europäischen Union (EU) in die USA bzw. nach China, was einen rechtmäßigen Übermittlungsmechanismus gemäß Art. 45 oder Art. 46 DSGVO erforderlich macht. Für die USA besteht mit dem EU-US Data Privacy Framework ein Angemessenheitsbeschluss nach Art. 45 DSGVO, s.u. 3.1.

Da zwischen der EU und China kein Datenschutzabkommen bzw. kein Angemessenheitsbeschluss der Europäischen Kommission besteht, stützt sich TikTok bei der Übermittlung personenbezogener Daten aus der EU nach China auf Standardvertragsklauseln. Keine EU-Datenaufsichtsbehörde hat den Übermittlungsmechanismus von TikTok bislang ausdrücklich als DSGVO-konform bestätigt. Im Gegenteil: Die irische Datenschutzbehörde stellte am 02.05.2025 fest, dass TikTok nicht ausreichend nachweisen konnte, dass die eingesetzten Standardvertragsklauseln und ergänzenden Maßnahmen bei Datenübermittlungen nach China ein mit der EU vergleichbares Datenschutzniveau gewährleisten. Sie verhängte ein Bußgeld von insgesamt 530 Mio. EUR – 485 Mio. EUR für die unzulässigen Übermittlungen (Art. 46 DSGVO) und 45 Mio. EUR für Transparenzverstöße (Art. 13 DSGVO) – und ordnete an, die Verarbeitung binnen sechs Monaten rechtskonform auszugestalten. Der Irish High Court hat die Vollstreckung wesentlicher Anordnungen am 13. November 2025 vorläufig ausgesetzt; die Übermittlungen nach China dauern daher bis zur gerichtlichen Klärung an. TikTok muss die Nutzenden hierüber per Hinweis in der App informieren.

Organisationen sollten daher vor der beruflichen Nutzung von TikTok eine spezifische Datenschutz-Folgenabschätzung durchführen. Ergibt diese Prüfung, dass die Plattform für die jeweilige Aufgabenerfüllung erforderlich ist und keine datenschutzfreundlicheren Alternativen mit geringerem Risiko zur Verfügung stehen, muss dies sorgfältig dokumentiert werden. Dadurch kann

im Falle einer Prüfung nachgewiesen werden, dass die datenschutzrechtlichen Risiken vor dem Einsatz der Plattform angemessen bewertet und berücksichtigt wurden.[1]

3.1 Datenschutzabkommen zwischen der EU und den USA

Am 11. Juli 2023 ist mit dem EU-US Data Privacy Framework ein Datenschutzabkommen zwischen der Europäischen Union und den USA in Kraft getreten.

Für die Arbeit in sozialen Medien ist das Abkommen besonders relevant, da die Verarbeitung europäischer Nutzendendaten durch große US-Social-Media-Plattformen in der Regel weiterhin in den USA stattfindet. In dem Abkommen wird festgelegt, dass die Vereinigten Staaten ein angemessenes Schutzniveau für personenbezogene Daten gewährleisten, die im Rahmen des Data Privacy Frameworks aus der EU an US-Unternehmen übermittelt werden. So soll sichergestellt werden, dass die Daten von Europäer*innen in den USA ein vergleichbares Schutzniveau genießen wie in der EU. Dennoch gibt es eine Reihe von Aspekten, die Unternehmen beachten sollten, um personenbezogene Daten zu schützen.

Mehr Informationen zum Datenschutzabkommen finden Sie hier: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv%3AOJ.L_.2023.231.01.0118.01.DEU&toc=OJ%3AL%3A2023%3A231%3AFULL.

3.2 Datenschutz-Folgenabschätzung (DSFA)

Eine Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO ist erforderlich, wenn die Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt. Vorrangig zu prüfen sind die von den deutschen Aufsichtsbehörden nach Art. 35 Abs. 4 DSGVO veröffentlichten Listen von Verarbeitungsvorgängen, für die eine DSFA zwingend durchzuführen ist („Muss-Listen"). Ergänzend benennen die Leitlinien der Artikel-29-Datenschutzgruppe (WP 248 rev.01), die der Europäische Datenschutzausschuss (EDSA) bestätigt hat, neun Kriterien. Sind mindestens zwei davon erfüllt, ist regelmäßig von einem hohen Risiko auszugehen. Für die Nutzung sozialer Medien sind insbesondere folgende Kriterien relevant:

- Systematische Überwachung öffentlich zugänglicher Bereiche
    - » Die Nutzung von Facebook Insights bzw. der Meta Business Suite Analytics umfasst die systematische Erfassung und Auswertung des Nutzerverhaltens von Besuchenden einer Seite. Dadurch kann dieses Kriterium erfüllt sein.

[1] Vgl. Entscheidung der irischen Datenschutzbehörde (DPC) vom 02.05.2025 zu Datenübermittlungen von TikTok nach China sowie die Anforderungen der Art. 5 Abs. 2 und 35 DSGVO.

- Umfangreiche Verarbeitung personenbezogener Daten
    - » Dieses Kriterium kann erfüllt sein, wenn eine Social-Media-Präsenz regelmäßig eine große Anzahl von Personen erreicht und deren Daten verarbeitet werden.
- Verarbeitung sensibler oder höchstpersönlicher Daten
    - » Bei Kanälen zu Themen wie Gesundheit, Sucht, Gewalt, Migration, Religion oder sexueller Orientierung lässt bereits das Folgen des Kanals, ein „Gefällt mir" oder ein Kommentar Rückschlüsse auf besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO zu.
- Datentransfers in Drittstaaten
    - » Die Nutzung von Facebook, Instagram, YouTube und LinkedIn ist regelmäßig mit der Übermittlung personenbezogener Daten in die USA verbunden. Bei TikTok können zudem Datenübermittlungen nach China erfolgen. Drittlandübermittlungen zählen nicht zu den neun Kriterien der Leitlinien, sind aber als eigenständiger Risikofaktor in die Bewertung einzubeziehen.

Eine DSFA sollte darstellen: welche personenbezogenen Daten verarbeitet werden, ob die Verarbeitung im Hinblick auf den verfolgten Zweck notwendig und verhältnismäßig ist (Art. 35 Abs. 7 lit. b DSGVO), welche Risiken für die betroffenen Personen bestehen, welche technischen und organisatorischen Maßnahmen zur Risikominderung getroffen wurden und ob das verbleibende Restrisiko als vertretbar angesehen werden kann.

Ergibt die DSFA, dass trotz aller Schutzmaßnahmen weiterhin ein hohes Risiko besteht, verpflichtet Art. 36 DSGVO den Verantwortlichen, vor Beginn der Datenverarbeitung die zuständige Datenschutzaufsichtsbehörde zu konsultieren.

Die Leitlinien der Europäischen Kommission zur Datenschutz-Folgenabschätzung (DSFA) finden Sie hier: https://ec.europa.eu/newsroom/article29/items/611236.

3.3 Gemeinsame Verantwortlichkeit

Seit mehreren Jahren steht Meta, insbesondere die Plattform Facebook, im Fokus datenschutzrechtlicher Diskussionen. Einen wichtigen Meilenstein stellte das Urteil des Europäischen Gerichtshofs (EuGH) vom 5. Juni 2018 (Rechtssache C-210/16, „Wirtschaftsakademie") dar. Darin entschied der EuGH, dass Betreibende einer Facebook-Seite[2] gemeinsam mit Facebook für die Verarbeitung personenbezogener Daten der Besuchenden der

[2] Facebook-Seiten werden auch Facebook-Fanpages oder Facebook-Pages genannt. Dabei handelt es sich um Benutzerkonten, die bei Facebook von Privatpersonen oder Unternehmen zu Präsentationszwecken und zur Einbringung von Äußerungen aller Art eingerichtet werden können.

Seite verantwortlich sind.[3] Damit begründete das Gericht eine gemeinsame datenschutzrechtliche Verantwortlichkeit zwischen Facebook und den jeweiligen Seitenbetreibenden.

Die Entscheidung hat erhebliche Auswirkungen auf die datenschutzrechtlichen Pflichten von Organisationen, Unternehmen und öffentlichen Stellen, die Facebook-Seiten betreiben. Sie sind nicht lediglich Nutzende der Plattform, sondern tragen Mitverantwortung für bestimmte Verarbeitungen personenbezogener Daten, die im Zusammenhang mit dem Besuch ihrer Seite erfolgen.

Das Gericht entschied dabei aber nicht, dass die Betreibenden von Facebook-Seiten für jeden datenschutzrechtlichen Verstoß von Facebook oder für jede Verarbeitung der Daten der Besuchenden von Facebook-Seiten haften. Die sogenannte „gemeinsame Verantwortlichkeit" bezog sich lediglich auf die Mitverantwortung im Hinblick auf die Bildung von „Insights-Statistiken"[4], die allen Facebook-Seiten-Betreibenden von Facebook zur Verfügung gestellt werden.

Die Entscheidung des EuGHs bezieht sich zwar auf einen Sachverhalt aus dem Jahr 2011 und betrifft die Rechtslage vor dem Inkrafttreten der DSGVO. Die Argumente des EuGHs können jedoch ohne Weiteres auf die DSGVO übertragen werden, da die DSGVO ebenfalls eine gemeinsame Verantwortlichkeit vorsieht. Das mit diesem EuGH-Urteil zusammenhängende deutsche Gerichtsverfahren ist im November 2021 mit Urteil rechtskräftig entschieden und abgeschlossen worden, wobei sich die deutschen Verwaltungsgerichte den Vorgaben des EuGH angeschlossen haben.

Wenn es sich um die „gemeinsame Verantwortlichkeit" im Sinne der DSGVO handelt, findet sich die gesetzliche Regelung in Art. 26 DSGVO. Dort ist unter anderem eine Verpflichtung der gemeinsam Verantwortlichen zum Abschluss einer Vereinbarung zu finden, in der festgelegt wird, wer welche Aufgaben und Pflichten übernimmt. Eine solche Vereinbarung bietet Meta unter dem Eintrag „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen" an; sie gilt auch für professionelle Instagram-Konten.[5] In dieser legt Meta fest, primär für die Verarbeitung der Daten der Seitenbesuchenden zur Erstellung der Insights-Statistiken verantwortlich zu sein und auch die o. g. Informations- und Auskunftspflichten zu erfüllen. Dazu müssen Seitenbetreibende Nutzer-

[3] Pressemitteilung Nr. 81/18 vom 5. Juni 2018 des Gerichtshofes der Europäischen Union; verfügbar unter: https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-06/cp180081de.pdf (18.06.2018).

[4] Unter „Facebook Insights" können Betreibende einer Facebook-Seite ihre Statistiken abrufen und analysieren. Alle Nutzenden, die als Administrator*innen einer Facebook-Seite eingetragen sind, haben Zugriff auf diese Informationen. Mithilfe dieses Werkzeugs können Aktivitäten der eigenen Seite ausgewertet werden, Erkenntnisse über die Zielgruppe (z. B. Alter, Geschlechterverteilung), über Abonnent*innen-Aktivitäten und die Verbreitung der eigenen Beiträge gewonnen werden.

[5] https://www.facebook.com/legal/terms/page_controller_addendum (25.04.23)

und Behördenanfragen unverzüglich, spätestens jedoch innerhalb von sieben Tagen an Meta weiterleiten.

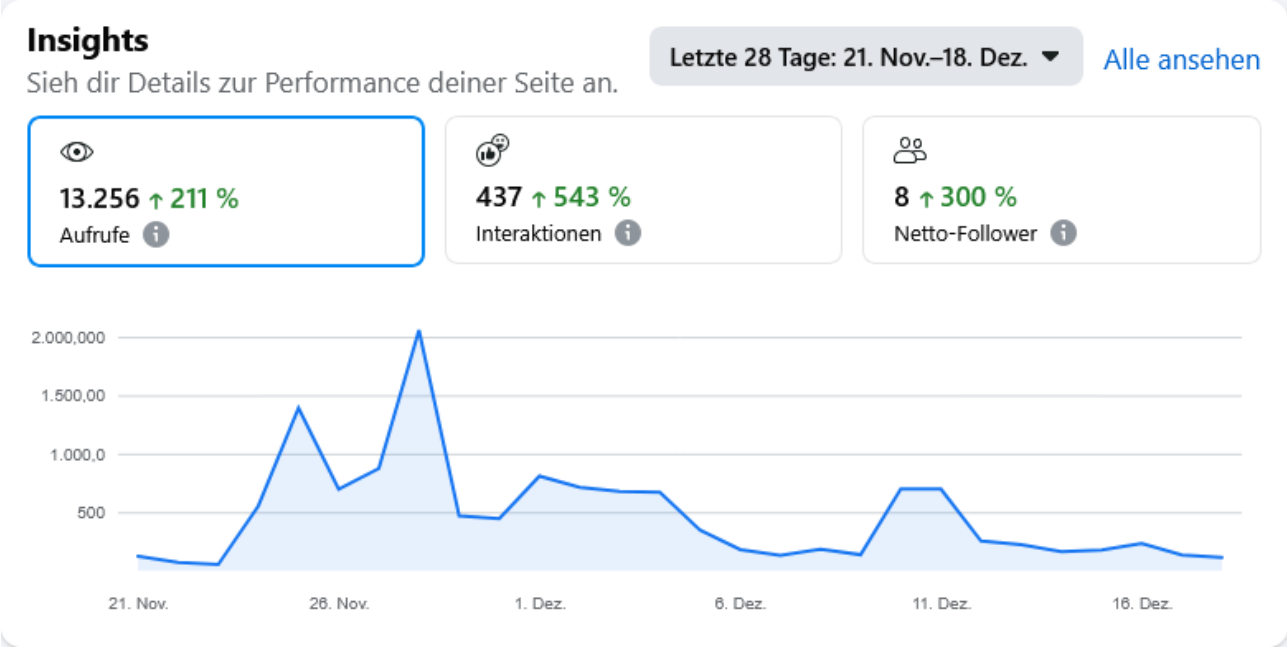

Abbildung 1: Beispiel für eine Insights-Statistik für Facebook-Seiten
Beispiel der Insights-Statistik für die Facebook-Seite „Social Media Bridge“, Bildschirmaufnahme von Dezember 2025 © Minor

In den vergangenen Jahren hat sich die Rechtsprechung zur gemeinsamen Verantwortlichkeit von Betreibenden von Facebook-Seiten weiterentwickelt. Dabei wurde insbesondere die Frage aufgegriffen, unter welchen Voraussetzungen Betreibende datenschutzrechtlich für Datenverarbeitungsvorgänge von Meta mitverantwortlich sein können.

Neuere Gerichtsentscheidungen setzen sich zunehmend damit auseinander, ob Betreibende einer Facebook-Seite tatsächlich Einfluss auf die Zwecke und Mittel der betreffenden Datenverarbeitung nehmen können. Fehlt es an einer solchen Einflussmöglichkeit, wird eine gemeinsame Verantwortlichkeit nicht ohne Weiteres angenommen. So haben deutsche Gerichte in jüngeren Verfahren hervorgehoben, dass die bloße Nutzung einer Facebook-Seite durch Betreibende noch nicht ausreicht, um eine gemeinsame datenschutzrechtliche Verantwortlichkeit für sämtliche Datenverarbeitungsvorgänge von Meta zu begründen.[6]

[6] Die vollständigen Entscheidungen des OVG Schleswig-Holstein vom 25.11.2021 (Az. 4 LB 20/13: https://www.gesetze-rechtsprechung.sh.juris.de/bssh/document/NJRE001490265) sowie des VG Köln vom 17.07.2025 (Az. 13 K 1419/23:

Für die Praxis bedeutet dies, dass die Frage der gemeinsamen Verantwortlichkeit weiterhin anhand der konkreten Umstände des Einzelfalls zu beurteilen ist. Beratungsanbietende und andere Organisationen, die Social-Media-Plattformen nutzen, sollten daher die weitere Entwicklung der Rechtsprechung aufmerksam verfolgen und die datenschutzrechtliche Ausgestaltung ihrer Online-Präsenzen regelmäßig überprüfen.

4. Was im Hinblick auf Datenschutz in den sozialen Medien zu beachten ist

1. **Durchführung einer Datenschutz-Überprüfung** von Online-Diensten, Social-Media-Plattformen und Tools
2. **Anpassung** der eigenen **Datenschutzerklärung** und **Online-Präsenzen**
3. **Anpassung** der **Einstellungen für KI-Training**

Mit der aktiven Nutzung neuer Online-Dienste, Social-Media-Plattformen oder Tools sollte erst begonnen werden, nachdem die Schritte 1 bis 3 abgeschlossen wurden.

4.1 Schritt 1: Datenschutz-Überprüfung

Vor der Einführung oder Nutzung einer Social-Media-Plattform oder eines Messenger-Dienstes sollte eine strukturierte datenschutzrechtliche Überprüfung durchgeführt werden. Ziel dieser Prüfung ist es, die mit dem Einsatz des jeweiligen Dienstes verbundenen Datenverarbeitungen zu identifizieren, deren Rechtmäßigkeit zu bewerten und mögliche datenschutzrechtliche Risiken frühzeitig zu erkennen. Die folgenden Fragen können dabei als Orientierung dienen:

Frage 1: Erfolgt bei der Nutzung der ausgewählten Social-Media-Plattform bzw. des Messenger-Dienstes eine Verarbeitung personenbezogener Daten?

Frage 2: Welche konkreten Zwecke rechtfertigen die Nutzung der Social-Media-Plattform bzw. des Messenger-Dienstes?

Frage 3: Kann das angestrebte Ziel auch ohne den Einsatz dieser Social-Media-Plattform bzw. dieses Messenger-Dienstes erreicht werden? Falls nicht, aus welchen Gründen?

---

https://nrwe.justiz.nrw.de/ovgs/vg_koeln/j2025/13_K_1419_23_Urteil_20250717.html) sind hier abrufbar. Die Entscheidungen befassen sich unter anderem mit der Frage, unter welchen Voraussetzungen eine gemeinsame datenschutzrechtliche Verantwortlichkeit von Betreibenden von Facebook-Fanpages und Meta angenommen werden kann.

Frage 4: Stellt die Social-Media-Plattform bzw. der Messenger-Dienst einen Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO oder eine Vereinbarung über die gemeinsame Verantwortlichkeit nach Art. 26 DSGVO zur Verfügung?

Frage 5: Werden durch die Social-Media-Plattform bzw. den Messenger-Dienst personenbezogene Daten in Staaten außerhalb der EU verarbeitet? Befindet sich der Anbieter außerhalb der EU oder werden entsprechende Unterauftragnehmer eingesetzt?

Frage 6: Bietet die Social-Media-Plattform bzw. der Messenger-Dienst Einstellungen oder Auswahlmöglichkeiten, die eine möglichst datensparsame und sichere Verarbeitung personenbezogener Daten ermöglichen? Falls ja, welche Optionen stehen zur Verfügung? Falls nein, bitte begründen.

4.2 Schritt 2: Datenschutzerklärung und Online-Präsenzen

Es sollte unbedingt darauf geachtet werden, dass auf allen Profilen und Seiten in den sozialen Medien die Datenschutzerklärung **hinterlegt bzw. verlinkt** ist. Der Wortlaut der Datenschutzerklärung soll dabei für jedes Vorhaben individuell angepasst werden, da Art und Umfang der Datenverarbeitung und -speicherung je nach Projekt variieren können. Ob sich Projekte im Hinblick auf den Zweck der Datenverarbeitung auf Art. 6 Abs. 1 lit. f DSGVO berufen können, wird unterschiedlich beurteilt; nach der hier vertretenen Auffassung erscheint dies grundsätzlich vertretbar.

Gemäß der DSGVO haben Einzelpersonen u. a. folgende Rechte: Auskunft (Art. 15), Berichtigung (Art. 16), Löschung (Art. 17), Einschränkung der Verarbeitung (Art. 18) und Widerspruch (Art. 21). Die Datenschutzerklärung einer Organisation sollte eine klare Kontaktstelle für Anfragen von betroffenen Personen enthalten (eine E-Mail-Adresse oder ein Kontaktformular, nicht nur eine allgemeine Anfrageadresse). Organisationen sollten über einen internen Prozess verfügen, um Anfragen innerhalb der Frist des Art. 12 DSGVO zu bearbeiten (ein Monat, verlängerbar auf drei Monate).

Hinweis: Das Kontaktieren über den Messengerdienst einer Plattform (z. B. Facebook Messenger), um ein Betroffenenrecht auszuüben, gilt als gültiges Ersuchen und muss entsprechend bearbeitet werden.

Im Folgenden werden die Möglichkeiten zur Einbindung der Datenschutzerklärung am Beispiel von Facebook-Profilen und -Seiten dargestellt. Da Facebook derzeit keine speziell für Datenschutzerklärungen vorgesehene Einbindungsmöglichkeit bereitstellt, handelt es sich hierbei um pragmatische Lösungsansätze.

Auf einem **Facebook-Profil** kann die Datenschutzerklärung an folgenden Stellen eingefügt werden:

- als Link im Steckbrief bzw. der Bio (siehe Abbildung 2) und

- als Foto mit dem Text der Datenschutzerklärung bzw. mit dem Link zu der Datenschutzerklärung als Bildbeschreibung (siehe Abbildung 3),
- als auf dem Profil oben fixierter Beitrag.

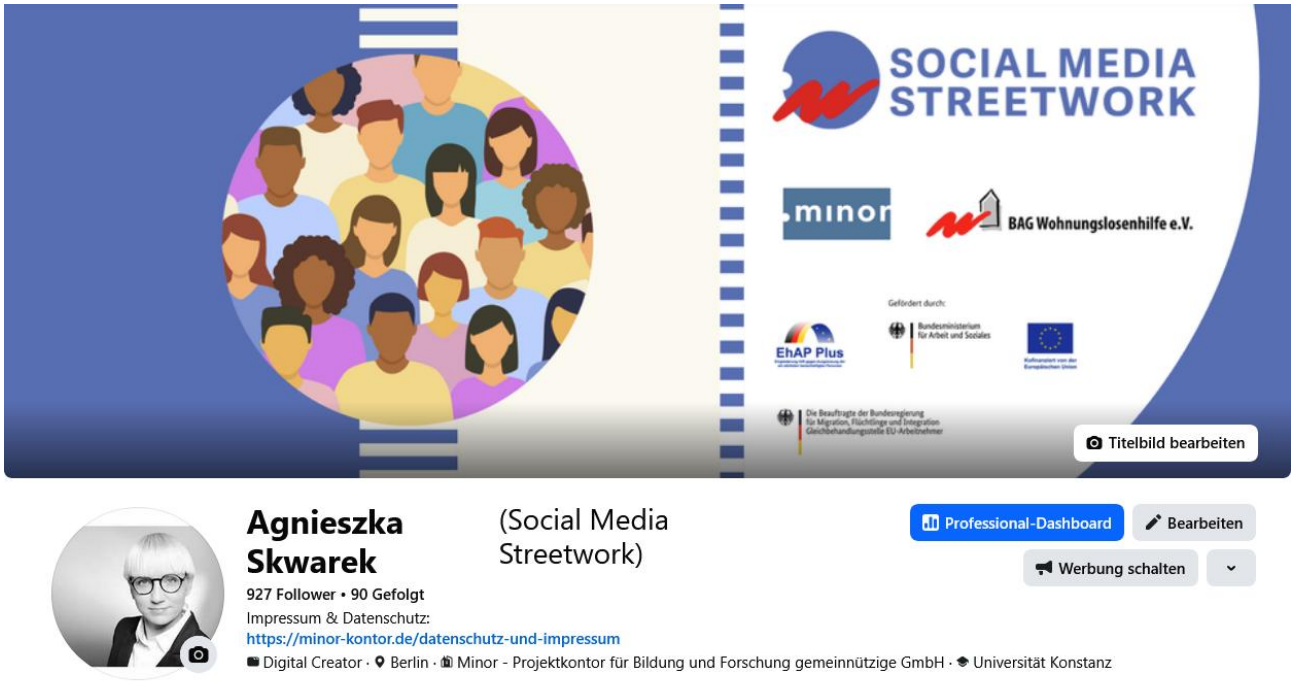

Abbildung 2: Datenschutzerklärung auf einem beruflichen Facebook-Profil
Bildschirmaufnahme des Profils einer Projektberaterin von Dezember 2019 © Minor

Abbildung 3: Foto mit dem Text der Datenschutzerklärung als Bildbeschreibung
Bildschirmaufnahme des Profils einer Projektberaterin von Dezember 2025 © Minor

Wenn es um **Facebook-Seiten** geht, kann der Link zur Datenschutzerklärung:

- unter dem Feld „Info/Datenrichtlinie“ platziert werden,
- statt der Webseite angegeben werden (z. B. „http://.../datenschutz “) und
- unter dem Feld „Story“ platziert werden.
- Alternativ besteht die Möglichkeit, den Datenschutzhinweis als Beitrag zu veröffentlichen und ihn oben auf der Seite oben zu fixieren.

Wichtig: Die Links zum Datenschutz und Impressum sollen immer anklickbar sein. Links, die nicht aktiv bzw. anklickbar sind, können die Auffindbarkeit der Pflichtinformationen erschweren und sollten daher vermieden werden.

Wenn auf der Plattform die Einbindung nur eines Links möglich ist:

- sollte ein gemeinsamer Impressums/Datenschutz-Links, wie z. B. https://minor-kontor.de/datenschutz-und-impressum/ oder
- z. B. Pastely bzw. ein anderes vergleichbares Tool genutzt werden, das die Verlinkung mehrerer Webseiten über einen zentralen Link im Profil ermöglicht: https://www.pastely.eu/.

- Die Links sollen anklickbar sein (vgl. oben) und es soll sich dabei um sog. sprechende Links handeln. Sprechende Links oder URLs sind Webadressen, die statt kryptischer Zeichenfolgen lesbare, natürlichsprachliche Begriffe enthalten, die den Inhalt der Seite beschreiben (z. B. https://minor-kontor.de/datenschutz/ oder https://minor-kontor.de/impressum/).

Bei den oben dargestellten Möglichkeiten zur Einbindung der Datenschutzerklärung und des Datenschutzhinweises bei Facebook handelt es sich ausschließlich um Vorschläge, die nach bestem Wissen und Gewissen auf Basis der bisherigen Rechtsprechung erstellt wurden. Es kann nicht ausgeschlossen werden, dass beispielsweise seitens Datenschutzbehörden abweichende Ansichten vertreten werden. In diesem Zusammenhang erscheint eine kontinuierliche Beobachtung der Rechtsprechung sowie eine regelmäßige Anpassung der Datenschutzerklärung und des Datenschutzhinweises notwendig.

Die oben dargestellten Möglichkeiten zur Einbindung von Datenschutzerklärungen können in der Regel auf weitere Social-Media-Plattformen übertragen werden. Jede Plattform bietet allerdings andere Möglichkeiten zur Einbindung von Inhalten an, sodass es in jedem Einzelfall notwendig ist, eine individuelle Lösung für die jeweilige Plattform zu erarbeiten. Abbildung 4 zeigt beispielhaft eine mögliche Lösung für die Darstellung einer Datenschutzerklärung auf einem beruflich genutzten Instagram-Profil.

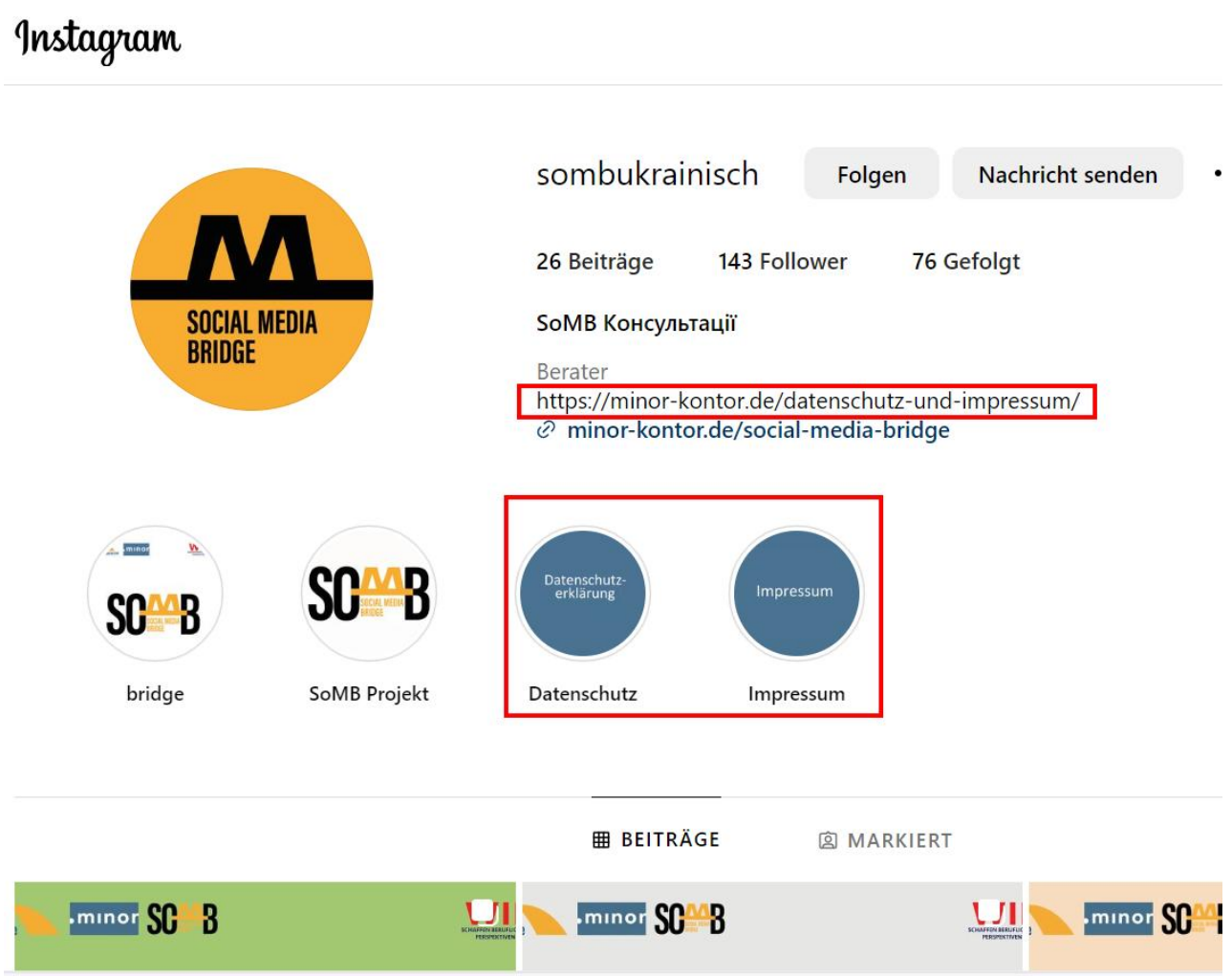

Abbildung 4: Datenschutzerklärung auf einem beruflichen Instagram-Profil
Bildschirmaufnahme des Profils eines Projekts von November 2023 © Minor

4.3 Schritt 3: KI-Training

LinkedIn, TikTok, YouTube und Meta (Facebook und Instagram) nutzen öffentlich sichtbare Inhalte auf ihren Plattformen, um ihre KI-Modelle zu trainieren. Dies betrifft Inhalte, die von Seitenbetreibenden gepostet werden (Beiträge einer Organisation, Fotos, Bildunterschriften, Kommentare), sowie öffentliche Kommentare, die Nutzende auf einer Seite hinterlassen. Die Nutzung öffentlich sichtbarer Inhalte für KI-Trainingszwecke erfolgt je nach Plattform auf unterschiedlicher Rechtsgrundlage und mit unterschiedlichen Widerspruchs- bzw. Einstellungsmöglichkeiten. Bei Meta und LinkedIn stützen sich die Anbieter auf ihr berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO); die Verarbeitung ist voreingestellt aktiv und kann nach Art. 21 DSGVO durch Widerspruch (Opt-out) beendet werden.

Hinweis: Ein Widerspruch (Opt-out) löscht keine Daten, die bereits für das Training verwendet wurden, und verhindert nicht, dass öffentliche Beiträge anderer Nutzender über die Organisation verwendet werden. Er gilt grundsätzlich nur für Inhalte, die von der Organisation selbst veröffentlicht wurden, nicht jedoch für Inhalte oder Kommentare, die eigenständig von anderen Nutzenden veröffentlicht werden. Damit die Daten der Nutzenden geschützt sind, müssen diese selbst widersprechen.

Laut dem Tätigkeitsbericht 2025 der Berliner Beauftragten für Datenschutz und Informationsfreiheit[7] bleibt ein Widerspruch gegen KI-Training grundsätzlich auch dann wirksam, wenn das geplante Training zunächst ausgesetzt, verändert oder erst später durchgeführt wird. Ein einmal erklärter Widerspruch bleibt in diesen Fällen grundsätzlich wirksam.

Die folgenden Schritte können auch in die Datenschutzerklärung aufgenommen werden, um Nutzende beim Schutz ihrer Daten zu unterstützen. Eine Begründung verlangen Meta und LinkedIn in ihren Formularen nicht. Wird dennoch ein Grund abgefragt, genügt der Hinweis auf das Widerspruchsrecht nach Art. 21 DSGVO.

Facebook

Einstellungen & Privatsphäre > Privacy Center > Weitere Richtlinien und Artikel > So verwendet Meta Informationen für generative KI-Modelle und -Funktionen > Datenschutz und generative KI – auf „Hier kannst du mehr darüber erfahren und Anfragen stellen“ klicken, die Eingabeaufforderungen ausfüllen und absenden.

Direktlink zu den Formularen: https://www.facebook.com/help/contact/510058597920541

Instagram

Der einfachste Weg, der Nutzung personenbezogener Daten für das KI-Training durch Instagram zu widersprechen, ist die Nutzung des entsprechenden Formulars: https://help.instagram.com/contact/767264225370182

TikTok

TikTok scheint derzeit keine In-App-Einstellung anzubieten, mit der sich das KI-Training deaktivieren lässt. Nutzende können jedoch ihr Widerspruchsrecht nach der DSGVO ausüben, indem sie einen entsprechenden Antrag über TikToks Datenschutzformular einreichen: https://www.tiktok.com/legal/report/privacy/webform/de

[7] https://www.datenschutz-berlin.de/jahresbericht-2025#B-IV-4

LinkedIn

Profilbild > Einstellungen & Datenschutz > Datenschutz > Daten zur Verbesserung generativer KI > „Ihre Daten zum Schulen von KI-Modellen verwenden, um Inhalte zu erstellen“ – auf Aus stellen.

Youtube

Creator und Rechteinhaber können auf YouTube über die Einstellung „Verwendung durch Drittunternehmen“ festlegen, ob Unternehmen ihre öffentlich zugänglichen YouTube-Videos zum Trainieren von KI-Modellen verwenden dürfen. Diese Einstellung ist standardmäßig deaktiviert (Opt-in). Wer nicht möchte, dass seine Inhalte von Drittunternehmen für KI-Training genutzt werden, muss daher nichts unternehmen. Unabhängig davon untersagen die YouTube-Nutzungsbedingungen die unbefugte Nutzung von Inhalten, etwa durch nicht autorisierten Download oder Scraping.

Für das KI-Training durch Google/YouTube selbst besteht dagegen keine Widerspruchsmöglichkeit; Grundlage ist die in den Nutzungsbedingungen eingeräumte Lizenz. Inhalte, die nicht für Trainingszwecke verwendet werden sollen, sollten daher nicht öffentlich auf YouTube veröffentlicht werden. Kommentare von Nutzenden werden von der Studio-Einstellung nicht erfasst.

Direkter Link zur YouTube-Hilfe „Deine Inhalte und die Verwendung durch Drittunternehmen": https://support.google.com/youtube/answer/15509945?hl=de.

Telegram

Telegram[8] erklärt, dass das Unternehmen nur die Daten speichert, die es benötigt, um einen sicheren und funktionsreichen Messenger-Dienst anzubieten. Es hat kein KI-Trainingsprogramm angekündigt, bei dem Nutzerdaten verwendet werden.

Zu beachten ist jedoch, dass Telegram seit 2025 den Chatbot Grok des Anbieters SpaceXAI integriert. Eingaben in direkter Interaktion mit Grok verlassen den Telegram-Kontext; für diese Daten gelten die Bestimmungen von SpaceXAI.

5. Weitere Nutzungs- und Einstellungsvorschläge

Viele Social-Media-Plattformen übermitteln Daten in Drittländer, darunter Meta (Facebook und Instagram), LinkedIn, Telegram und TikTok. Das Schutzniveau unterscheidet sich dabei erheblich: Für Übermittlungen in die USA besteht mit dem EU-US Data Privacy Framework ein

[8] Telegram ist kein klassischer Social-Media-Dienst, wird in diesem Dokument jedoch mitbetrachtet, da über Telegram-Kanäle und -Gruppen häufig spezifische Zielgruppen erreicht und adressiert werden.

Angemessenheitsbeschluss, für Übermittlungen nach China nicht, s.o. Unabhängig davon, ob ein Datenschutzrahmen besteht oder das Unternehmen seinen Sitz in der EU hat und dort reguliert wird, werden zusätzliche Maßnahmen empfohlen, um die Nutzung personenbezogener Daten zu begrenzen. Im Folgenden werden Möglichkeiten vorgestellt, die von diesen Plattformen erhobenen Daten zu begrenzen.

5.1 Schutz der Privatsphäre und Moderation von Inhalten

Organisationen sollten die Privatsphäre der Nutzenden auf ihren Kanälen schützen. Die Möglichkeiten sind dabei plattformabhängig: Auf Facebook-Seiten lässt sich die Liste der Personen, denen die Seite gefällt bzw. die ihr folgen, in den Seiteneinstellungen ausblenden. Auf Instagram ist dies bei professionellen Konten nicht möglich – Follower-Listen öffentlicher Konten sind grundsätzlich einsehbar. Wo die Zugehörigkeit zur Followerschaft selbst eine sensible Information darstellt (z. B. bei Beratungsangeboten zu Aufenthaltsrecht, Gesundheit oder Gewalt), sollte dies bei der Kanalwahl und in der Datenschutzerklärung ausdrücklich berücksichtigt und kommuniziert werden. Außerdem empfiehlt es sich, klare Regeln für die Kommentarspalten zu erstellen. Kommentare, in denen Nutzende unerlaubt sensible Daten von sich oder Dritten posten (z. B. Telefonnummern, Herkunft, rechtliche Probleme), müssen aktiv moderiert oder gelöscht werden.

Temporäre Inhalte beispielsweise Stories auf Instagram und Facebook verschwinden nach 24 Stunden aus der Sicht der Nutzenden, Meta behält jedoch die zugrunde liegenden Daten. Temporäre Inhalte hinterlassen dauerhafte Datenspuren. Wenn personenbezogene Daten in einer Story erscheinen, gelten dieselben Datenschutzpflichten wie für einen dauerhaften Beitrag.

5.2 Risiken von Messengerdiensten

Beim Umgang mit sensiblen Daten ist es am besten, Messengerdienste zu verwenden, die Ende-zu-Ende-verschlüsselt sind. Nachrichten sind auf Instagram, LinkedIn oder TikTok nicht Ende-zu-Ende-verschlüsselt. Auf Instagram bestand bis zum 8. Mai 2026 eine optional zuschaltbare Ende-zu-Ende-Verschlüsselung; Meta hat diese Funktion weltweit abgeschaltet. Seither greift dort nur noch eine Transportverschlüsselung, bei der Meta den Schlüssel besitzt und Inhalte – einschließlich Bildern, Videos und Sprachnachrichten – serverseitig auswerten kann. TikTok hat erklärt, eine Ende-zu-Ende-Verschlüsselung für Direktnachrichten sei derzeit nicht geplant. Auf Facebook sind Nachrichten zwischen privaten Nutzenden seit Dezember 2023 standardmäßig Ende-zu-Ende-verschlüsselt, Nachrichten mit Unternehmenskonten jedoch nicht. In Telegram sind nicht alle Chats standardmäßig Ende-zu-Ende-verschlüsselt. Diese ist nur für geheime Chats aktiviert. Nachrichten, die in normalen Cloud-Chats gesendet werden, werden mit einer Client-Server-Verschlüsselung verschlüsselt, die weniger sicher ist, und die Nachrichten werden auf den Servern von Telegram gespeichert.

Insbesondere bei sensiblen Daten sollte dies bei der Nutzung von Messengerdiensten berücksichtigt werden. Zudem sollte geprüft werden, ob die Nutzung eines Business-Accounts auf Facebook zwingend erforderlich ist. Besondere Aufmerksamkeit verdient zudem der Instagram-Direktnachrichtenkanal: Da dort seit Mai 2026 keine Ende-zu-Ende-Verschlüsselung mehr verfügbar ist, ist er für vertrauliche Kommunikation weniger geeignet als der Facebook Messenger zwischen privaten Konten. Wenn die erste Kontaktaufnahme über den Instagram Direktnachrichtenkanal, Facebook Messenger oder ähnliches erfolgt, sollte möglichst auf sicherere Dienste wie beispielsweise Signal[9] oder Präsenzberatungsangebote gewechselt werden. Bei Signal lässt sich seit 2024 ein Benutzername anstelle der Telefonnummer verwenden, sodass ratsuchende Personen ihre Rufnummer nicht offenlegen müssen; dies senkt die Hürde für einen Wechsel. In der Praxis ist es jedoch erfahrungsgemäß unwahrscheinlich, dass eine ratsuchende Person auf eine andere Plattform wechselt, was eine Hürde für den Datenschutz in der aufsuchenden Beratung darstellt.

Organisationen können neben den privaten Nachrichten auch Messenger-Kanäle oder -Gruppen nutzen, um mit Zielgruppen zu kommunizieren. Administrator*innen eines Kanals bzw. einer Gruppe sind für dessen Ausgestaltung datenschutzrechtlich mit verantwortlich. Dies betrifft insbesondere die durch die Teilnahme selbst entstehen (Benutzernamen, sichtbare Telefonnummern, Profilfotos und die Teilnahme an der Gruppe) sowie die von der Organisation selbst veröffentlichten Inhalte. Für Inhalte, die Mitglieder eigenständig posten, bestehen Moderations- und Vorsorgepflichten. Eine alleinige Verantwortlichkeit der Administrator*innen für sämtliche fremden Inhalte lässt sich der Rechtslage dagegen nicht entnehmen. In Betracht kommt eine gemeinsame Verantwortlichkeit mit dem Plattformbetreiber nach Art. 26 DSGVO, wie sie der EuGH für Facebook-Fanpages angenommen hat (Urteil vom 5. Juni 2018, C-210/16). Für rein private Gruppen ohne organisatorischen Bezug greift dagegen die Haushaltsausnahme nach Art. 2 Abs. 2 lit. c DSGVO.

Es ist wichtig zu beachten, dass die hier sowohl von der Organisation als auch von den Gruppenmitgliedern geteilten Daten überwacht bzw. abgegriffen werden können. Öffentliche Gruppen und Kanäle sind am wenigsten sicher, da sie über das Internet vollständig abrufbar sind. Eine private Gruppe mit einem offenen Einladungslink ist zwar weiterhin auffindbar und jedermann kann eintreten; die Inhalte der Gruppe können jedoch nur diejenigen sehen, die der Gruppe zuerst beigetreten sind. Ob neu beitretende Mitglieder den bisherigen Chatverlauf

[9] Signal nutzt Ende-zu-Ende-Verschlüsselung und verfolgt das Prinzip der Datensparsamkeit. Der Dienst verarbeitet und speichert nur wenige personenbezogene Daten. Da Signal als US-amerikanischer Anbieter Infrastruktur und Dienstleister in den USA nutzt, können personenbezogene Daten in die USA übertragen werden. Für solche Datenübermittlungen sind die datenschutzrechtlichen Anforderungen der DSGVO an internationale Datentransfers zu beachten.

einsehen können, ist bei Telegram eine Einstellungssache und sollte bewusst konfiguriert werden. So kann in den Gruppeneinstellungen festgelegt werden, dass der Verlauf für neue Mitglieder verborgen bleibt. Dies ist eine der wirksamsten und zugleich am einfachsten umzusetzenden Schutzmaßnahmen.

Zusätzlich zur Beschränkung der geteilten Informationen auf nicht sensible Daten sollten Vorsichtsmaßnahmen zugunsten der Gruppenmitglieder getroffen werden. Die Möglichkeit für Gruppenmitglieder, Nachrichten zu senden, kann deaktiviert werden, wodurch verhindert wird, dass sie potenziell sensible Daten weitergeben. Der Gruppenchat dient in diesem Fall ausschließlich als Informationskanal. Ist hingegen ein offener Austausch zwischen den Mitgliedern gewünscht, können Administrator*innen das Versenden bestimmter Arten von Inhalten (z. B. Dateien, Fotos, Links) gezielt einschränken. Ergänzend empfiehlt es sich, die Sichtbarkeit der Mitgliederliste einzuschränken, soweit der Dienst dies zulässt, und Mitglieder darauf hinzuweisen, dass ihre bei der Registrierung hinterlegte Telefonnummer je nach Privatsphäre-Einstellung für andere Gruppenmitglieder sichtbar sein kann.

Die Nutzenden sollten vor dem Beitritt über die Datenerhebung informiert werden. Bei Facebook und Instagram sollte die Datenschutzerklärung in den Profilen und auf den Seiten gespeichert bzw. verlinkt sein, wie in Abschnitt 4.2 erläutert. Bei WhatsApp-Business-Konten sowie bei allen Telegram-Konten kann in der Regel ein Link zur Datenschutzerklärung im Profil hinterlegt werden. Bei WhatsApp Business sowie bei Telegram Business- und Premium-Konten kann zudem eine automatische Begrüßungsnachricht eingerichtet werden. Diese kann beispielsweise einen Hinweis auf die Datenschutzerklärung und einen entsprechenden Link enthalten. Bei privaten WhatsApp-Konten besteht hingegen keine Möglichkeit, einen Link zur Datenschutzerklärung im Profil zu hinterlegen oder eine automatische Begrüßungsnachricht zu versenden. Eine Nachricht mit einem Datenschutzhinweis (einschließlich der Namen der Gruppenbetreiber, welche Daten verarbeitet werden, sowie eines Links zur Datenschutzerklärung) sollte angeheftet werden, damit alle Nutzenden sie beim Beitritt sehen. Zudem kann es sinnvoll sein, für Gruppen eine Administratorfreigabe zu verlangen. Personen, die einen Beitritt zur Gruppe beantragen, kann zunächst der Datenschutzhinweis zugesandt werden, und sie können der Gruppe erst beitreten, wenn sie diesen gelesen und ihm zugestimmt haben.

Zusammenfassend werden für Datenschutzhinweise in Messengerdiensten die folgenden Maßnahmen empfohlen:

1. Bereitstellung eines Datenschutzhinweises auf der Webseite oder in dem Formular, über das die Kontaktdaten oder der Einladungslink zur Gruppe veröffentlicht werden
2. Verlinkung der Datenschutzerklärung im Konto- bzw. Profiltext, soweit dies möglich ist

3. Bei Gruppenchats: Verlinkung der Datenschutzerklärung in der Gruppenbeschreibung und/oder in einer angehefteten Nachricht
4. Bei Direktnachrichten: Bereitstellung eines Links zur Datenschutzerklärung in einer Begrüßungsnachricht
5. Hinweis darauf, welche Inhalte über den jeweiligen Kanal nicht geteilt werden sollten (z. B. Angaben zu Aufenthaltsstatus oder rechtlichen Verfahren), verbunden mit dem Angebot eines sichereren Kanals
6. Dokumentation der getroffenen Einstellungen (Sichtbarkeit des Chatverlaufs, Sendeberechtigungen, Beitrittsfreigabe) im Verarbeitungsverzeichnis, damit die Maßnahmen im Prüfungsfall nachweisbar sind

5.3 Statistiken und Analysen

Viele Social-Media-Plattformen, darunter Facebook, Instagram, LinkedIn und TikTok, erheben automatisch Daten über Seitenbesuchende und stellen Betreibenden von Seiten oder Profilen aggregierte Statistiken und Analysen zur Verfügung. Es werden demografische Daten (Alter, Geschlecht, Standort), Verhaltensdaten (z. B. Seitenaufrufe, Interaktionen und Verweildauer) sowie Reichweitendaten erfasst. In vielen Fällen kann diese Datenerhebung durch die Betreibenden nicht vollständig deaktiviert werden. Es empfiehlt sich, regelmäßig zu prüfen, welche Analysefunktionen für die jeweilige Arbeit tatsächlich erforderlich sind, und diese, soweit möglich, auf das notwendige Maß zu beschränken oder auf ihre Auswertung zu verzichten. Der Verzicht auf die Nutzung beseitigt die Verantwortlichkeit zwar nicht, ist aber im Rahmen der Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO ein relevantes Argument und sollte dokumentiert werden.

Darüber hinaus können Organisationen prüfen, ob für ihre Kommunikationsziele die Nutzung eines persönlichen Profils anstelle einer Seite bzw. eines Business-Accounts ausreichend ist. Die jeweilige Plattform erhebt und verarbeitet auch in diesem Fall weiterhin Daten über Besuchende. Je nach Plattform können sich jedoch Umfang und Verfügbarkeit von Analyse- und Statistikfunktionen unterscheiden. Dabei ist zu berücksichtigen, dass Plattformen von Organisationen häufig die Nutzung von Seiten oder Business-Accounts erwarten.

5.4 Eingebettete Widgets auf Webseiten

Viele Social-Media-Kanäle bieten Widgets an, die in die Webseite einer Organisation eingebettet werden können, beispielsweise Facebook-Like-/Share-Buttons, LinkedIn-Buttons oder YouTube-Videos. Solche Widgets können bereits beim Laden der Webseite Daten über die Besuchenden an die jeweilige Plattform übermitteln, selbst wenn die Besuchenden dort kein Benutzerkonto besitzen oder nie mit dem Widget interagieren. Nach dem EuGH-Urteil vom 29.07.2019 (C-40/17,

„Fashion ID") ist die einbindende Webseite für diese Übermittlung mitverantwortlich. Unabhängig davon verlangt § 25 Abs. 1 TDDDG (bis Mai 2024: TTDSG) für das Speichern von Informationen auf dem Endgerät und den Zugriff darauf eine vorherige Einwilligung.

Nach Möglichkeit sollten Textlinks anstelle von Widgets verwendet werden. Textlinks lösen keine Datenübermittlung aus und sind damit die einzige vollständig einwilligungsfreie Lösung. Schaltflächen oder Widgets sollten nicht auf der eigenen Webseite einer Organisation eingebunden werden, ohne eine Zwei-Klick-Lösung zu implementieren (bei der die Schaltfläche erst aktiviert wird, nachdem Nutzende bewusst darauf geklickt haben, um sie zu aktivieren).

Wenn YouTube-Videos auf einer eigenen Webseite eingebettet werden, sollte in der Einbettungs-URL „youtube-nocookie.com“ anstelle von „youtube.com“ verwendet werden. Dadurch kann die Datenübermittlung an Google vor dem Abspielen des Videos reduziert werden, auch wenn sie nicht vollständig ausgeschlossen wird.

5.5 Datennutzung für Werbeschaltungen

Standortdaten werden von Social-Media-Plattformen über die Standortdienste von Endgeräten (z. B. GPS, WLAN- und Mobilfunkortung), sofern die Nutzenden der App den Zugriff erlaubt haben, sowie standardgemäß über IP-Adressen und über von Nutzenden bereitgestellte Standortdaten erhoben und für Personalisierungs- und Werbezwecke genutzt. Diese Daten werden zusammen mit Informationen über Interessen und Aktivitäten von Nutzenden für Werbezwecke bereitgestellt.

Um den Datenschutz, gegeben der Möglichkeiten, zu maximieren, können Organisationen beim Schalten kostenpflichtiger Werbung (selbst beim „Boosten“[10] eines Beitrags) auf die Nutzung von verhaltensbasiertem oder detailliertem Targeting verzichten. Es sollte nur grobes geografisches oder sprachbasiertes Targeting verwendet werden.

Technische Umsetzung im Meta -Werbeanzeigenmanager:

1. Im Werbeanzeigenmanager oder in der Business Suite zum Bereich Zielgruppe navigieren
2. Unter Standorte lediglich die grobe Region (z. B. das Land, Bundesland oder Stadt) festlegen
3. Unter Sprachen die gewünschte Sprache auswählen

[10] Auf Facebook bedeutet „einen Beitrag boosten“, dass man einen bereits veröffentlichten Beitrag gegen Bezahlung bewirbt, damit er mehr Menschen angezeigt wird.

4. Das Feld „Detailliertes Targeting“ (Interessen, Demografie, Verhalten) freilassen
5. Die gewählten Einstellungen dokumentieren und in das Verarbeitungsverzeichnis aufnehmen, damit die Datenminimierung nachweisbar ist

Soziale Medien, digitale Kommunikationsformen und die zugehörigen datenschutzrechtlichen Anforderungen unterliegen einem fortlaufenden Wandel. Als *living document* wird diese Arbeitshilfe regelmäßig an relevante Entwicklungen angepasst. Die dargestellten Hinweise und Empfehlungen basieren auf dem Prinzip des Privacy by Design. Wo sie keine konkrete Antwort bietet, kann dieses Prinzip als wichtige Orientierung für die datenschutzkonforme Ausgestaltung von Prozessen, Einstellungen und Arbeitsweisen dienen.

Fachstelle Einwanderung und Integration

Minor – Projektkontor für Bildung und Forschung gGmbH
Alt-Reinickendorf 25, 13407 Berlin

Tel.: +49 (0)30 457989504
E-Mail: fei@minor-kontor.de

www.minor-kontor.de
www.netzwerk-iq.de/einwanderung.html

Stand: 18.08.2026

Das Förderprogramm IQ – Integration durch Qualifizierung zielt mit Unterstützung des Europäischen Sozialfonds Plus (ESF Plus) auf die nachhaltige Verbesserung der Arbeitsmarktintegration von Erwachsenen ausländischer Herkunft ab. Der ESF Plus ist Europas wichtigstes Instrument zur Förderung von Beschäftigung und sozialer Integration in Europa. Deutschland erhält in der ESF Plus-Förderperiode 2021-2027 rund 6,56 Mrd. Euro. Davon fließen rund 2,22 Mrd. Euro in das ESF Plus-Bundesprogramm und rund 4,34 Mrd. Euro in die ESF Plus-Aktivitäten der Bundesländer.

Weitere Infos zum ESF Plus unter: www.esf.de.

Weitere Infos zum Förderprogramm IQ unter: www.netzwerk-iq.de.

Die Fachstelle Einwanderung und Integration wird im Rahmen des Förderprogramms IQ – Integration durch Qualifizierung durch das Bundesministerium für Arbeit und Soziales und die Europäische Union über den Europäischen Sozialfonds Plus (ESF Plus) gefördert und vom Bundesamt für Migration und Flüchtlinge administriert. Partner in der Umsetzung sind das Bundesministerium für Bildung, Familie, Senioren, Frauen und Jugend und die Bundesagentur für Arbeit.

Gefördert durch: Bundesministerium für Arbeit und Soziales; Kofinanziert von der Europäischen Union
Administriert durch: Bundesamt für Migration und Flüchtlinge
In Kooperation mit: Bundesministerium für Bildung, Familie, Senioren, Frauen und Jugend; Bundesagentur für Arbeit

Die Fachstelle Einwanderung und Integration wird zusätzlich finanziert durch die Bundesagentur für Arbeit sowie die Senatsverwaltung für Arbeit, Soziales, Gleichstellung, Integration, Vielfalt und Antidiskriminierung aus Landesmitteln, die das Abgeordnetenhaus von Berlin beschlossen hat.

Bundesagentur für Arbeit
Senatsverwaltung für Arbeit, Soziales, Gleichstellung, Integration, Vielfalt und Antidiskriminierung
BERLIN