

I AGREE

...to what I see

Informations-Visualisierung von
Social-Media-Datenschutzrichtlinien

Bewusstseinsbildung durch visuelle Simplifizierung

Sabrina Melojer

I AGREE... to what I see

Informationsvisualisierung von Social-Media-Datenschutzrichtlinien – Bewusstseinsbildung durch visuelle Simplifizierung

MASTERARBEIT

Eingereicht von

Sabrina Melojer, BA

Durchgeführt an der FH Vorarlberg (www.fhv.at)
Master-Studiengang InterMedia

Betreut von

Prof. (FH) Dipl. Des. (FH) Michael Kneidl
Prof. (FH) Dipl. -Ing. Dr. techn. Karl-Heinz Weidmann

Dornbirn, im Juli 2023

Kurzfassung

In einer Zeit allgegenwärtiger Online-Interaktionen sind Datenschutzbedenken für Nutzer:innen von sozialen Medien und Messenger-Diensten zu einem wichtigen Thema geworden. Obwohl es wichtig ist, die Inhalte von Datenschutzrichtlinien bzw. Datenschutzerklärungen zu erfassen, haben Benutzer:innen Schwierigkeiten, den Umfang, die komplexe Rechtssprache und die technischen Details in diesen Dokumenten zu verstehen. Dies führt dazu, dass sie sich diesen Datenschutzrisiken, die mit ihren Online-Aktivitäten verbunden sind, nicht bewusst sind.

Diese Masterarbeit beschäftigt sich mit der Frage, inwieweit Informationen von Social-Media-Datenschutzrichtlinien durch eine einheitliche Struktur einem breiten Nutzer:innenkreis leichter zugänglich gemacht werden können. Diese sollen dabei nicht nur gekürzt, sondern durch den Einsatz gestalterischer Mittel vereinfacht, sprich simplifiziert, werden, ohne den jeweiligen Inhalt zu verfälschen. Die Studie wird einen benutzer:innenzentrierten Designansatz verwenden, der die Zusammenarbeit von Teilnehmer:innen mit unterschiedlichen demografischen Merkmalen und unterschiedlichen technologischen Kompetenzniveaus beinhaltet. Durch einen iterativen Prozess wird ein Zeichensystem in Form verschiedener Icons entworfen, verfeinert und bewertet, um die effektivsten Formate für die Übermittlung von Datenschutzinformationen zu ermitteln. Hierbei spielen wahrnehmungspsychologische Aspekte eine wesentliche Rolle.

Um die Auswirkungen der Visualisierungen auf das Bewusstsein und das Verständnis der Datenschutzerklärungen der Benutzer:innen zu bewerten, wird ein gemischter Methodenansatz eingesetzt. Quantitative Daten werden durch Befragungen vor und nach der Intervention gesammelt, um das Wissen und Verständnis der Teilnehmer:innen über Datenschutzkonzepte zu bewerten. Darüber hinaus werden durch Interviews und der Erstellung sowie des Testings eines Prototypens quali-

tative Daten gesammelt, um tiefere Einblicke in die Wahrnehmungen und Erfahrungen der Teilnehmer:innen zu gewinnen. Für die Umsetzung des Prototypens ist eine Webseite angedacht, die Nutzer:innen einen Überblick der wichtigsten Inhalte der Datenschutzrichtlinien ermöglicht und in reduzierter Form, durch den Einsatz von Icons, darstellt (z. B. Was wird gesammelt? Welche Risiken sind damit verbunden? usw.). Die Ergebnisse dieser Forschungsarbeit werden zum Bereich der Informationsvisualisierung beitragen, indem sie Strategien ermöglicht, um komplexe Datenschutzerklärungen zu vereinfachen und sie für Nutzer:innen sozialer Medien und Messenger-Dienste zugänglicher zu machen. Durch die Förderung des Bewusstseins und des Verständnisses für Datenschutzpraktiken soll die Zielgruppe in die Lage versetzt werden, fundierte Entscheidungen bezüglich ihrer persönlichen Daten zu treffen und Datenschutzrisiken zu mindern. Die Entwicklung benutzer:innenfreundlicher bzw. menschenzentrierter Datenschutznchnittstellen fördert dabei nicht nur die Transparenz, sondern auch das Vertrauen in neue Technologien und Medien.

Zusammenfassend setzt sich diese Masterarbeit mit der entscheidenden Herausforderung, das Datenschutzbewusstsein durch Vereinfachung und Visualisierung von Datenschutzrichtlinien sozialer Medien zu stärken. Durch die Kombination von Prinzipien der Informationsvisualisierung mit den teils schwer zugänglichen Inhalten dieser Texte versucht diese Arbeit, die Lücke zwischen dem Verständnis/Bewusstsein der Nutzer:innen und den rechtlichen Komplexitäten zu schließen und letztendlich eine datenschutzbewusstere digitale Gesellschaft zu fördern.

Schlüsselwörter: Datenschutzrichtlinie, Soziale Medien, Messenger-Dienste, Informationsvisualisierung, Zeichensystem, Bewusstsein, Icons

Abstract

In today's digital era of ubiquitous online interactions, the use of social media and messenger services has raised major concerns about privacy. Although it is important to capture the content of privacy policies respectively data protection declarations, users grapple with the sometimes complex scope, legal jargon and technical terminology. As a result, users are left uninformed and unaware of the privacy risks associated with their online activities.

The objective of this master thesis is to design and evaluate simplified visual representations of social media privacy statements that effectively communicate the key privacy concepts to users. These should not only be shortened, but simplified through the use of design means, without distorting the respective content. A user-centered design approach will be adopted, involving iterative design cycles and feedback from participants with varying levels of technological proficiency. The central objective is to develop effective visualization strategies that can transform complex privacy statements into intuitive and accessible visual representations, fostering awareness and empowering users to make informed decisions about their online privacy. Psychological aspects of perception play a major part here.

The study will employ a mixed-methods research methodology. Quantitative data will be collected through pre- and post-intervention surveys to assess participants' knowledge and understanding of privacy concepts. Qualitative data will be gathered through interviews and the creation and usability testing of a prototype to obtain insights into users' perceptions and experiences with the visualized privacy statements. A website is planned for the implementation of the prototype, which gives users an overview of the most important content of the privacy policies and presents them in a reduced form through the use of icons (e.g. What is collected? What risks are associated with it? etc.).

The findings of this research will contribute to the field of information visualization by offering strategies to simplify complex privacy statements and make them more accessible for users of social media and messenger services. By raising awareness and facilitating comprehension of privacy statements, the thesis seeks to empower users to exercise their privacy rights and make informed choices about their online presence. The development of user-friendly and human-centric privacy interfaces not only enhance the clarity and transparency, but ultimately foster a trust-based relationship with users.

In summary, this master thesis addresses the critical challenge of enhancing privacy awareness through the simplification and visualization of social media privacy statements. By combining principles of information visualization with the intricacies of privacy policies, the research seeks to bridge the gap between users' understanding and the legal complexities of online privacy, ultimately fostering a more privacy-conscious digital society.


Keywords: privacy policies, social media, messenger services, information visualization, awareness, icons



Inhaltsverzeichnis

Kurzfassung	005
Abstract	006
Inhaltsverzeichnis	007
Abbildungsverzeichnis	011
Tabellenverzeichnis	012
Anhangsverzeichnis	013
Abkürzungsverzeichnis	013
1. Einleitung	015
1.1 Erkenntnisinteresse und Fragestellungen	016
1.2 Forschungsstand und Methodik	017
1.3 Aufbau und Gliederung	018
2. Theoretischer Bezugsrahmen	022
2.1 Datenschutz im Social-Web	022
2.1.1 Datenschutzrecht Österreich und EU	022
2.1.1.1 Österreichisches Datenschutzgesetz	023
2.1.1.2 EU-Datenschutzgrundverordnung	023
2.1.2 Datenschutzrichtlinien sozialer Medien	024
2.1.2.1 Meta Platforms Inc. (Facebook, Instagram)	024
2.1.2.2 Twitter	025
2.1.2.3 TikTok	026
2.1.2.4 LinkedIn	026

2.1.2.5	WhatsApp	027
2.1.2.6	Signal	027
2.2	Informationswahrnehmung und Interpretation	028
2.2.1	Wahrnehmung von Informationen	028
2.2.1	Wahrnehmung und Vermittlung durch Zeichen	029
2.2.3	Simplifizierung durch Text-Visualisierung	031
2.3	Konzeption eines informationsgrafischen Systems	033
2.3.1	Konzept der Semiotik: Begriffsdefinition und Abgrenzung	033
2.3.1.1	Definition Symbol, Index, Ikon, Piktogramm	034
2.3.1.2	Ikonizitätsgrade	036
2.3.2	Entwicklung eines Zeichensystems	036
2.3.2.1	Grundlagen und Überlegungen	037
2.3.2.2	Übertragung von Kategorien in Zeichensystem	037
2.3.2.3	Konzept Icon-Design	037
2.4	Prototyp: I AGREE to what I see	038
2.4.1	Aufbau und Inhalt	038
2.4.2	Entwürfe und Skizzierung	039
2.4.3	Erstellung Click-Dummy	041
3.	Methodisches Vorgehen und Analyse	048
3.1	Befragung zur Nutzung sozialer Medien	048
3.1.1	Methodenwahl	048
3.1.2	Ablauf	051
3.1.3	Auswertung und Ergebnisse	051



3.2	Textanalyse nach Datenkategorien DSGVO	055
3.2.1	Methodenwahl	055
3.2.2	Ablauf	055
3.2.3	Auswertung und Ergebnisse	056
3.3	Cluster-Analyse	057
3.3.1	Methodenwahl	057
3.3.2	Ablauf	058
3.3.3	Auswertung und Ergebnisse	059
3.4	Icon-Erstellung und Testing	062
3.4.1	Erste Entwürfe und Überlegungen	062
3.4.2	Umsetzung	063
3.4.1	Methodenwahl	065
3.4.2	Ablauf	065
3.4.3	Auswertung und Ergebnisse	065
3.5	Testing Click-Dummy	069
3.5.1	Methodenwahl	069
3.5.2	Ablauf	069
3.5.3	Auswertung und Ergebnisse	071
4.	Interpretation und Diskussion	074
4.1	Befragung	074
4.2	Textanalyse	075
4.3	Cluster-Analyse	076
4.4	Icon-Design	077
4.5	Click-Dummy	077

5. Conclusio und Ausblick	080
Literaturverzeichnis	084

Abbildungsverzeichnis

- Abbildung 1 Sicherheit Datensammlung (TikTok Datenschutzerklärung, 2022)
- Abbildung 2 Teilen von Informationen (WhatsApp Datenschutzrichtlinie, 2022)
- Abbildung 3 Saussures Model des sprachlichen Zeichens (Nöth, 2000, S.74)
- Abbildung 4 Skizze Grundidee (Eigene Darstellung, 2021)
- Abbildung 5 Skizze Vorgehen Prototyp (Eigene Darstellung, 2021)
- Abbildung 6 Paper-Prototyp (Eigene Darstellung, 2021)
- Abbildung 7 Skizze Seitenaufbau Click-Dummy (Eigene Darstellung, 2022)
- Abbildung 8 Startseite Click-Dummy (Figma, eigene Darstellung, 2023)
- Abbildung 9 Startseite Detail Click-Dummy (Figma, eigene Darstellung, 2023)
- Abbildung 10 Navigation Über Click-Dummy (Figma, eigene Darstellung, 2023)
- Abbildung 11 Navigation Datenschutz Click-Dummy (Figma, eigene Darstellung, 2023)
- Abbildung 12 Navigation Datensammler Click-Dummy (Figma, eigene Darstellung, 2023)
- Abbildung 13 Detailseite Was wird gesammelt? Click-Dummy (Figma, eigene Darstellung, 2023)
- Abbildung 14 Detailseite Gesichtserkennung Click-Dummy (Figma, eigene Darstellung, 2023)
- Abbildung 15 Fragebogen zur Nutzung sozialer Medien (Eigene Darstellung, 2022)
- Abbildung 16 Auszug Datenschutzrichtlinien TikTok (TikTok Datenschutzrichtlinie, 2022)
- Abbildung 17 Cluster Dendrogramm (Eigene Darstellung, 2022)
- Abbildung 18 Entwürfe Icons Gesundheitsdaten, Standortdaten, Biometrische Daten, Gesichtserkennung und Persönliche Daten (von l. nach r., eigene Darstellung, 2022)
- Abbildung 19 Gesichtserkennung Icon 1 (eigene Darstellung, 2022)
- Abbildung 20 Gesichtserkennung Icon 2 (Eigene Darstellung, 2022)
- Abbildung 21 Gesichtserkennung Icon 3 (Eigene Darstellung, 2022)
- Abbildung 22 Biometrische Daten Icon 1 (Eigene Darstellung, 2022)
- Abbildung 23 Biometrische Daten Icon 2 (Eigene Darstellung, 2022)
- Abbildung 24 Biometrische Daten Icon 3 (Eigene Darstellung, 2022)
- Abbildung 25 Kommunikationsüberwachung Icon 1 (Eigene Darstellung, 2022)
- Abbildung 26 Kommunikationsüberwachung Icon 2 (Eigene Darstellung, 2022)
- Abbildung 27 Kommunikationsüberwachung Icon 3 (Eigene Darstellung, 2022)
- Abbildung 28 Gesundheitsdaten Icon 1 (Eigene Darstellung, 2022)
- Abbildung 29 Gesundheitsdaten Icon 2 (Eigene Darstellung, 2022)
- Abbildung 30 Gesundheitsdaten Icon 3 (Eigene Darstellung, 2022)
- Abbildung 31 GPS & Standortüberwachung Icon 1 (Eigene Darstellung, 2022)
- Abbildung 32 GPS & Standortüberwachung Icon 2 (Eigene Darstellung, 2022)
- Abbildung 33 GPS & Standortüberwachung Icon 3 (Eigene Darstellung, 2022)
- Abbildung 34 Personenbezogene Daten Icon 1 (Eigene Darstellung, 2022)
- Abbildung 35 Personenbezogene Daten Icon 2 (Eigene Darstellung, 2022)
- Abbildung 36 Personenbezogene Daten Icon 3 (Eigene Darstellung, 2022)
- Abbildung 37 Profildaten Icon 1 (Eigene Darstellung, 2022)
- Abbildung 38 Profildaten Icon 2 (Eigene Darstellung, 2022)

Abbildung 39 Profildaten Icon 3 (Eigene Darstellung, 2022)

Abbildung 40 Technische Daten Icon 1 (Eigene Darstellung, 2022)

Abbildung 41 Technische Daten Icon 2 (Eigene Darstellung, 2022)

Abbildung 42 Technische Daten Icon 3 (Eigene Darstellung, 2022)

Abbildung 43 Usability-Testing Icons (Eigene Darstellung, 2022)

Abbildung 44 Ergebnis Icon-Testing (Eigene Darstellung, 2022)

Abbildung 45 Fragebogen Click-Dummy (Eigene Darstellung, 2023)

Abbildung 46 Datenschutzrichtlinie Instagram 2020 (Instagram Datenschutzrichtlinie, 2020)

Tabellenverzeichnis

Tabelle 1 Peirce' neun Subzeichenklassen (Nöth, 2000, S. 66)

Tabelle 2 LIX-Werte Datenschutzrichtlinien (Auswertung Psychometrica Lesbarkeits-Index, 2022)

Tabelle 3 Begriffe Card-Sorting (Datenschutzrichtlinien Meta - Facebook, Instagram, 2023; TikTok, 2022; LinkedIn, 2020; Twitter, 2022; Meta-WhatsApp, 2022; Signal, 2018; EU Verordnung 2016/679)

Tabelle 4 Auszug Cardsorting (Eigene Darstellung, 2022)

Tabelle 5 Cluster-Auswertung (Eigene Darstellung, 2022)

Tabelle 6 Auszug Auswertung Nutzer:innen-Kategorien (Eigene Darstellung, 2022)

Tabelle 7 Bewertungs-Schema Usability-Testing Icons (Eigene Darstellung, 2022)

Tabelle 8 Auswertung Usability-Testing Icons (Eigene Darstellung, 2022)



Anhangsverzeichnis

- 01 Fragebögen soziale Medien**
- 02 Textanalyse**
- 03 Cardsorting und Cluster-Analyse**
- 04 Icon Präferenz-Testing**
- 05 Prototyp und Auswertung**

Abkürzungsverzeichnis

BG	Bundesgesetz
DSG	Datenschutz-Gesetz
EG	Europäische Gemeinschaft
EU-DSGVO	Europäische Datenschutzgrundverordnung
LIX	Lesbarkeitsindex

„Privacy is dead, and social media hold the smoking gun.“

Pete Cashmore, Special to CNN

1. Einleitung

Soziale Medien sind nur nutzbar, wenn den jeweiligen Allgemeinen Geschäftsbedingungen (kurz AGBs) und somit den Datenschutzrichtlinien zugestimmt wurde. Obwohl die Zustimmung mit der Bestätigung erfolgt, diese gelesen zu haben, ist das meist nicht der Fall. Zu diesem Schluss kommt beispielsweise die im Jahr 2018 von der University of Connecticut durchgeführte Studie *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services* (Obar & Oeldorf-Hirsch, 2018). Darin gaben 97 Prozent der Teilnehmer:innen an, die Datenschutzrichtlinien nicht zu lesen. Als Begründung wurde sowohl der Umfang als auch die darin enthaltene Vielzahl an Informationen angegeben (Obar & Oeldorf-Hirsch, 2018).

Die am 1. Jänner 2023 in Kraft getretene Datenschutzrichtlinie des US-Technologiekonzerns Meta Platforms Inc., dem unter anderem die Produkte Facebook und Instagram angehören, umfasst beispielsweise neunundzwanzig DIN A4 Seiten (reiner Text, Schriftart Arial, Schriftgröße 10) und ca. 22.300 Wörter (Meta Datenschutzrichtlinie, 2023). Bei einer durchschnittlichen Lesezeit von 300 Wörtern pro Minute benötigen Leser:innen ca. 74 Minuten zum Lesen des gesamten Textes. Ein zeitlicher Aufwand, den, wie aus der zitierten Studie hervorgeht, ein großer Teil der Nutzer:innen nicht aufbringt.

Was vielen nicht bewusst ist, ist die Tatsache, dass sie sich durch die Bestätigung einer Fülle an Vertragsbedingungen unterwerfen und den jeweiligen Unternehmen persönliche Daten sowie Rechte zu deren Verarbeitung zur Verfügung stellen, was durchaus mit Risiken verbunden ist. Wie bereits erwähnt, ist das fehlende Datenschutzbewusstsein von Nutzer:innen häufig auf den Umfang der Datenschutzrichtlinien sowie deren erschwerte Zugänglichkeit zu den darin enthaltenen relevanten Informationen zurückzuführen. Die großen Konzerne, die diese Plattformen betrei-

ben, scheinen kein Interesse daran zu haben, Nutzer:innen über die Bedeutung und den Wert der einzelnen Daten aufzuklären. Denn ohne dieses Bewusstsein ist es sehr unwahrscheinlich, dass einzelne Personen Bedingungen in den Datenschutzrichtlinien hinterfragen oder etwa einen selbstbestimmteren Umgang mit ihren Daten einfordern. Veruschka Götz und Anna Rigamonti sprechen in ihrem Buch *Informationsvisualisierung - Missbrauch und Möglichkeit* von einem vorherrschenden Überangebot an Informationen, sodass „die eigentliche Information verdeckt und eine gezielte Informationsvermittlung verhindert“ (Götz & Rigamonti, 2015, S. 39) wird.

Die vorliegende Arbeit beschäftigt sich mit der Frage, inwieweit Informationen aus den Datenschutzrichtlinien ausgewählter Plattformen und Dienste durch den Einsatz gestalterischer Mittel wie Icons, dargestellt und vereinfacht, sprich simplifiziert, werden können, ohne den jeweiligen Inhalt zu verfälschen. Nutzer:innen sollen befähigt werden, bewusster mit ihren eigenen Daten und deren Schutz umzugehen und zu erfassen, wie weit ihre eigene Persönlichkeit und ihr Verhalten auf sozialen Medien sowie durch die Nutzung von Messenger-Diensten anhand hinterlassener Datenspuren ablesbar wird und wo mögliche Sicherheitsrisiken liegen, die zu großen finanziellen und/oder persönlichem Schaden führen können, falls die Daten für cyberkriminelle Zwecke missbraucht werden.

In einer qualitativen Inhaltsanalyse der Datenschutzrichtlinien von fünf sozialen Medien und zwei Messenger-Diensten sowie einer mit mehreren Nutzer:innen durchgeführten Befragung und Cluster-Analyse zeigen sich die dargelegten Probleme recht deutlich, was in einem späteren Teil dieser Arbeit noch ausführlicher beschrieben wird. Der Bereich der Netzpolitik in mehreren Ländern hat sich seit über 30 Jahren zum Ziel gesetzt, „dem Nutzer von Kindheit an bis ins hohe Alter eine hin-

reichende Aus- und Fortbildung über das gesamte Spektrum der Digitalmedien zu ermöglichen“ (Klumpp, 2020, S. 518).

Neben der Vermittlung von Medienkompetenz und Konzepten der Medienpädagogik soll Nutzer:innen demnach auch der Umgang mit sozialen Medien ermöglicht werden (Klumpp, 2020, S. 518). Die vorliegende Arbeit soll einen Beitrag dazu leisten, das Verständnis und Bewusstsein von Datenschutz und somit auch die Datenkompetenz in der Gesellschaft zu fördern.

1.1 Erkenntnisinteresse und Fragestellungen

Die Datenschutzrichtlinien vieler sozialer Medien und Messenger-Dienste sind aufgrund ihres Umfangs, der zum Teil verklausulierten Sprache sowie durch die Anordnung der Informationen für Nutzer:innen nur schwer zugänglich. Für sie relevante Informationen sind dadurch nicht zu erfassen. Dies ist teils auch gesetzlichen Verpflichtungen geschuldet, was die Betreiber allerdings nicht daran hindern würde, Nutzer:innen die relevantesten Inhalte zusätzlich in verkürzter Form zur Verfügung zu stellen.

In erster Linie geht in dieser Arbeit deshalb darum, diese Informationen sichtbar zu machen. Sie beschäftigt sich mit der Frage, inwieweit Informationen aus den Datenschutzrichtlinien durch den Einsatz gestalterischer Mittel dargestellt und vereinfacht (simplifiziert) werden können, ohne den jeweiligen Inhalt zu verfälschen.

Daraus ergibt sich die im Folgenden angeführte Hauptforschungsfrage dieser Arbeit sowie weitere damit zusammenhängende Unterforschungsfragen.

Forschungsfrage

Kann Informations-Design Nutzer:innen dabei unterstützen, ein Verständnis für den Datenschutz zu entwickeln?

Das Ziel dieser Arbeit ist herauszufinden, ob eine überlegte Reduktion von Informationen aus den Datenschutzrichtlinien sowie deren Übertragung in ein grafisches System Nutzer:innen befähigt, ein Verständnis und – damit einhergehend – ein Bewusstsein für den Datenschutz zu entwickeln. Relevante Informationen sollen nicht nur erfasst, sondern in ihrer Bedeutung richtig eingeordnet werden können – auch im Hinblick auf die mit einzelnen Daten verbundenen Risiken.


Für die theoretische Ausarbeitung und Beantwortung der Frage ist es erforderlich, grundlegende Vorgänge der Informationswahrnehmung zu beleuchten.

Unterforschungsfrage 1

Die Entwicklung eines Verständnisses des Datenschutzes ist ein Prozess, der von verschiedenen Faktoren abhängig ist. Daraus ergeben sich weitere Fragen, die im Zuge dieser Arbeit beantwortet werden sollen.

Wie weit muss der Inhalt von Datenschutzrichtlinien reduziert werden, damit dieser zugänglich und verständlich wird?

Aufgrund der Quantität der Datenschutzrichtlinien ist es notwendig, eine Reduktion der Informationen durch-, ohne dabei eine Verflachung herbeizuführen. Nach Götz und Rigmonti könnte letzteres unter anderem durch ein bewusstes Weglassen wichtiger Informationen sowie die grobe Zusammenfassung relevanter Inhalte passieren (Götz & Rigmonti, 2015, S. 142). Die Simplifizierung einer Information darf diese keinesfalls verfälschen oder deren inhaltliche Bedeutung ändern –



auch hinsichtlich der rechtlichen Vorgaben aus dem Datenschutzgesetz und der Datenschutzgrundverordnung. Die Auswahl, Organisation bzw. Kategorisierung sowie die Aufbereitung von thematischen Schwerpunkten aus den Datenschutzrichtlinien stehen hierbei im Vordergrund.

Unterforschungsfrage 2

Die zweite Unterforschungsfrage beschäftigt sich mit grafischen Aufbereitungsmöglichkeiten ausgewählter Informationen aus den Datenschutzrichtlinien. Die konkrete Frage lautet:

Welche Darstellungsformen sind für die Übertragung in ein informationsgrafisches System sinnvoll, um den Inhalt der Informationen verständlich darstellen zu können?

Zur Entwicklung geeigneter Zeichen (Icons) ist es notwendig, im Vorfeld die theoretischen Grundlagen und Hintergründe der Semiotik, Semantik und Pragmatik genauer zu beleuchten. Die Definition einzelner Begriffe sowie deren Beziehungen zueinander sind dabei von besonderer Relevanz.

1.2 Forschungsstand und Methodik

“The simplest way to achieve simplicity is through thoughtful reduction.”
(Maeda, 2006, S. 1)

Ein wesentlicher Schwerpunkt dieser Forschungsarbeit liegt in der überlegten Reduktion von Informationen aus den Datenschutzrichtlinien sowie deren Übertragung in ein grafisches System, das sich in das visuelle Gedächtnis von Nutzer:innen einprägt, um

so – im besten Fall – ein Datenschutzbewusstsein zu ermöglichen. Als literarisches Grundgerüst dient hierbei vor allem Jacques Bertins Standardwerk *Graphische Semiotik – Diagramme, Netze, Karten*, das grundlegende Vorgänge und Voraussetzungen für die Identifizierung, Registrierung, Vermittlung und Weiterverarbeitung von Informationen. Die grafische Aufbereitung von Informationen und deren Beziehungen zwischen bereits bekannten Begriffen stehen hierbei im Vordergrund.

Für die Theoriebildung zur Simplifizierung der Informationen der Datenrichtlinien wird das Werk von John Maeda *The Laws of Simplicity* herangezogen. Genannt seien hierbei insbesondere seine Analyseansätze SORT, LABEL, INTEGRATE und PRIORITIZE (Maeda, 2006, S. 13f). Mit *Informationsvisualisierung – Missbrauch und Möglichkeit* von Veruschka Götz und Anna Rigamonti soll zudem auch auf die Schwierigkeiten im Informationsdesign bei der Erstellung von Grafiken eingegangen werden. Da die Wahrnehmung eines Menschen einen erheblichen Einfluss auf die Aufnahme und Verarbeitung von Informationen hat, widmet sich ein Punkt dieser Arbeit den Theorien der (Wahrnehmungs-)Psychologen James J. Gibson und John M. Kennedy. Hierbei geht es vor allem darum, welche Fähigkeiten bei der Erfassung von visuellen Darstellungen eine Rolle spielen. Zur Theoriebildung der Entwicklung eines Zeichensystems werden unter anderem die Werke von Otl Aicher und Martin Krampen sowie von Adrian Frutiger herangezogen, um die Thematik von mehreren Blickwinkeln zu betrachten. Für das dafür ebenfalls notwendige Konzept der Semiotik und deren Begriffsdefinitionen dient das *Handbuch der Semiotik* von Winfried Nöth als Grundlage. Der Schwerpunkt liegt dabei auf den Theorien der Sprachwissenschaftler und Philosophen Ferdinand de Saussure und Charles Sanders Peirce.

Für die Erarbeitung der rechtlichen Grundlagen zu Beginn dieser Arbeit ist es zudem notwendig, die gesetzlichen Bestimmungen hinsichtlich des Datenschutzes (Datenschutzgesetz und Datenschutzgrundverordnung) genauer zu beleuchten. Abschließend sind an dieser Stelle die Werke von Edward Tufte, aber auch Andy Kirk zu erwähnen, da sie die Hintergründe und Prinzipien für gute Informationsvisualisierung darlegen. Letzterer hebt bei der Definition der Datenvisualisierung besonders hervor, dass diese darauf abzielen, das Verständnis zu erleichtern (Kirk, 2019, S. 20.), was in Bezug auf das Forschungsbestreben von besonderer Relevanz ist.

1.3 Gliederung und theoretische Grundlagen

Die Forschungsarbeit unterteilt sich in fünf Abschnitte. Der erste Teil widmet sich der allgemeinen Einführung in das Thema, der Erörterung des Problemhintergrundes und den Fragestellungen.

Im zweiten Kapitel erfolgt die Beleuchtung des theoretischen Bezugsrahmens, beginnend mit einer Analyse der rechtlichen Vorgaben und des Materials, also den Datenschutzrichtlinien ausgewählter sozialer Medien und Messenger-Dienste. Anschließend folgen unter Punkt 2.2 theoretische Grundlagen zur Informationswahrnehmung und Interpretation, also wahrnehmungspsychologische Aspekte und den notwendigen Prozessen für die Aufnahme und Verarbeitung von visuellen Darstellungen (Bilder, Zeichen). Der letzte Punkt des zweiten Abschnitts widmet sich der Konzeption eines informationsgrafischen Systems. Hier werden die Konzepte der Semiotik, die für die Entwicklung eines Zeichensystems, genauer gesagt der Icons, in dieser Arbeit von großer Relevanz sind, betrachtet.

Das dritte Kapitel beschäftigt sich mit dem methodischen Vorgehen der Forschungsarbeit. Der erste Teil dient der Erörterung der Nutzungsweise sozialer Medien und Messenger-Dienste von Nutzer:innen sowie deren Grundkenntnisse zum Thema Datenschutz. Aus einer Textanalyse der ausgewählten Datenschutzrichtlinien resultieren die Begriffe für ein darauffolgendes Cardsorting und der Benennung eigener Kategorien durch die Proband:innen, die durch eine Cluster-Analyse in die Erstellung eines Dendrogramms einfließen. Die daraus gewonnenen Ergebnisse bilden die Grundlage für die Gestaltungsansätze der Icons unter Punkt 3.4. Daraus ergeben sich erste Ansätze zur Beantwortung der (Unter-) Forschungsfragen. Zudem fließen diese in die Entwicklung und das Testing des Prototypens (Click-Dummy) unter Punkt 3.5 mit ein.

Im vierten Kapitel erfolgt die Diskussion und Interpretation der Ergebnisse aus den Befragungen, Analysen und Testings aus Kapitel drei. Aus den erarbeiteten Grundlagen und daraus gewonnenen Ergebnissen werden die notwendigen Rückschlüsse zur Beantwortung der Forschungsfragen gezogen.

Im letzten Punkt der Masterarbeit werden alle gewonnenen Erkenntnisse und Schlussfolgerungen zusammengefasst und dahingehend diskutiert, inwieweit das angestrebte Ziel der Erhöhung des Datenschutzbewusstseins durch das Forschungsvorhaben teilweise oder gänzlich erreicht werden konnte. Dabei soll auf mögliche zukünftige menschenzentrierte Gestaltungsansätze verwiesen werden.

„People are demanding that Facebook, Google and other platforms give them privacy, but it’s an even bigger issue than that. For the most part, big companies like Google and Facebook offer very little transparency into the data they collect and how they do so. People should be given control over which information the company can collect and use.“

Eli Pariser, entrepreneur, activist and author of *The Filter Bubble*

Theoretischer Bezugsrahmen

Datenschutz im Social-Web

Informationswahrnehmung und Interpretation

Konzeption eines informationsgrafischen Systems

Prototyp: I AGREE to what I see

2. Theoretischer Bezugsrahmen

Das Kapitel zum theoretischen Bezugsrahmen unterteilt sich in vier verschiedene Abschnitte. Zu Beginn werden die rechtlichen Grundlagen zum Thema Datenschutz besprochen. Anschließend erfolgt eine Analyse der sozialen Medien und Messenger-Dienste, deren Datenschutzrichtlinien in dieser Arbeit untersucht werden. Zudem werden Kritikpunkte und Probleme hinsichtlich Datenschutz aufgezeigt. Der zweite Abschnitt beschäftigt sich mit der Informationswahrnehmung, also wie Informationen generell verarbeitet werden können und welche Fähigkeiten dafür notwendig sind. Der dritte Teil widmet sich zu Beginn der Zeichentheorie. Darauf aufbauend erfolgen die Überlegungen zum Icon-Design, die für das Forschungsvorhaben entworfen werden. Der letzte Abschnitt des Kapitels widmet sich der Konzeption zur praktischen Umsetzung eines Klick-Dummies zu einer Webseite - *I AGREE to what I see*.

2.1 Datenschutz im Social-Web

Zur Erforschung des weiter oben beschriebenen Problems werden für die Analyse die Datenschutzrichtlinien von folgenden sozialen Medien und Messenger-Diensten untersucht: Facebook und Instagram, die inzwischen zu Meta Platforms gehören und deshalb in einer Richtlinie zusammengefasst sind, TikTok, LinkedIn, Twitter, Signal und WhatsApp (Anm.: WhatsApp ist ebenfalls ein Produkt von Meta Platforms, verfügt aber über eine eigene Datenschutzrichtlinie). Um auch die rechtlichen Grundlagen miteinzubeziehen, werden im ersten Schritt die Hintergründe zum Datenschutz, also zum österreichischen Datenschutzgesetz sowie zur EU-Datenschutzgrundverordnung, erläutert. Anschließend folgt eine Beschreibung der oben genannten Plattformen, deren Schwerpunkte sowie identifizierte Kritikpunkte

bezüglich des Datenschutzes.

2.1.1 Datenschutzrecht Österreich und EU

Der Schutz personenbezogener Daten hat in Österreich schon seit über 40 Jahren Tradition. Geregelt wird dieser über das Österreichische Datenschutzgesetz (kurz DSG) sowie über die Europäische Datenschutzgrundverordnung (kurz DSGVO). Als personenbezogene Daten gelten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Verordnung 2016/679 des Europäischen Parlaments und des Rates).

Durch Inkrafttreten letzterer am 25.05.2018 rückte das Thema Datenschutz vermehrt in den Fokus der Öffentlichkeit. Die Intention in Bezug auf die Verordnung war und ist unter anderem, mehr Datenschutz für natürliche Personen zu gewährleisten, indem ihnen mehr Rechte als Betroffene, beispielsweise Recht auf Auskunft, Berichtigung, Löschung usw., eingeräumt werden (Verordnung 2016/679 des Europäischen Parlaments und des Rates, Kapitel III). Zudem werden Unternehmen bei der Speicherung und Verarbeitung von Daten vermehrt in die Pflicht genommen und müssen bei Verstößen mit hohen Strafen rechnen. Aus rechtlicher Sicht haben die Verordnung und die zusätzliche Anpassung des österreichischen Datenschutzgesetzes für eine deutliche Verbesserung bezüglich des Missbrauchs von personenbezogenen Daten (Name, Geburtsdatum, Adresse usw.) gesorgt. Was damit nicht erreicht werden konnte, ist ein breites Verständnis oder Bewusstsein für Daten sowie deren Schutz in der Bevölkerung zu schaffen.

2.1.1.1 Österreichisches Datenschutzgesetz

Als einer der ersten Staaten in Europa hat Österreich im Jahr 1978 ein Datenschutzgesetz zum Schutz personenbezogener Daten erlassen und eine dazugehörige Behörde (damals Datenschutzkommission) ins Leben gerufen. Das Bundesgesetzblatt Nr. 565/1978 (565 Bundesgesetz: Datenschutzgesetz - DSG, 1978) legte in 59 Paragrafen bereits den Grundstein für den Schutz personenbezogener Daten und schuf somit ein Grundrecht auf Datenschutz für alle in Österreich lebenden Personen. Schon die damalige Fassung enthielt wesentliche Punkte zur Zulässigkeit der Ermittlung und Verarbeitung, Zulässigkeit der Übermittlung, Meldung der Verarbeitung, Pflicht zur Richtigstellung oder Löschung sowie zum Auskunftsrecht.

Mit der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates wurde am 24. Oktober 1995 das Datenschutzrecht und somit der „Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ für ganz Europa eingeführt (Richtlinie 95/46/EG, Europäisches Parlament, 1995).

Darauf aufbauend wurde im Jahr 2000 das Datenschutzgesetz (DSG 2000) in Österreich grundlegend überarbeitet und an die Richtlinie angepasst. Am 23. Mai 2013 wurde das bisherige Datenschutzgesetz erneut geändert und die Datenschutzkommission von der bis heute bestehenden Datenschutzbehörde mit Sitz in Wien abgelöst. Die Einführung der Europäischen Datenschutzgrundverordnung brachte erneute Änderungen für das Datenschutzgesetz mit sich. Diese waren allerdings so aufwändig, dass das Gesetz vollständig überarbeitet werden musste. Somit ist nunmehr das Bundesgesetz BGBl. I Nr. 120/2017 in Österreich gültig, das mit 25. Mai 2018 in Kraft getreten ist. Gemeinsam mit der DSGVO

bildet es die Grundlage für das Datenschutzrecht natürlicher Personen.

2.1.1.2 EU-Datenschutzgrundverordnung

Wie bereits weiter oben erwähnt, trat die EU-Datenschutzgrundverordnung (EU 2016/679) mit 25. Mai 2018 in Kraft. Sie dient dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr in der Europäischen Union. Sie löste die ehemalige Richtlinie 95/46/EG aus dem Jahr 1995 ab und berücksichtigt auch aktuelle Gegebenheiten wie soziale Netzwerke, Big Data, Internet der Dinge usw. In der DSGVO sind die grundlegenden Aspekte für das Datenschutzgesetz geregelt, wie beispielsweise Betroffenenrechte (Recht auf Auskunft, Richtigstellung, Löschung, Widerspruch). Zudem regelt sie die Anforderungen an Datenschutzrichtlinien von Webseitenbetreibern, Unternehmen, Plattformen usw. und teilt diese in Verantwortliche und Auftragsverarbeiter auf.

Besonders relevant in Hinblick auf die Richtlinien sozialer Medien ist der Artikel 9 der DSGVO, auf den in einem späteren Teil der Arbeit noch genauer eingegangen wird (Verordnung 2016/679 des Europäischen Parlaments und des Rates, Kapitel II, Artikel 9). Dieser regelt die persönlichen Daten, die als besonders schützenswert gelten und somit für Nutzer:innen mit besonderen Risiken verbunden sein können, falls diese für kriminelle Zwecke missbraucht werden.

Zur Beantwortung der Fragestellungen sind einzelne Inhalte der DSGVO von besonderer Relevanz, da diese den Nutzer:innen in verständlicher Form nähergebracht bzw. bewusst gemacht werden sollen.

2.1.2 Datenschutzrichtlinien sozialer Medien

Die DSGVO verpflichtet die Verantwortlichen und Auftragsverarbeiter – in diesem Sinne die Betreiber der sozialen Medien und Messenger-Dienste – ein Verzeichnis zu führen, in dem sie sämtliche Verarbeitungstätigkeiten offenlegen. Dies ist größtenteils in der jeweiligen Datenschutzrichtlinie festgehalten. Darunter fallen beispielsweise die Beschreibung der Kategorien der betroffenen Personen sowie die personenbezogenen Daten, Übermittlung der Daten, Rechtsauskunft zur Löschung Richtigstellung usw., allgemeine Beschreibungen zur Verarbeitung, Datenspeicherung, Tracking und vieles mehr. Die Verarbeitung darf zudem nur stattfinden, wenn dieser zugestimmt wurde – was mit einem Klick als Bestätigung recht einfach vonstatten geht. Trotz dieser Vorgaben stehen einige Unternehmen immer wieder aufgrund von Verstößen gegen das Datenschutzrecht in der Kritik. Die Datenschutzrichtlinien der in dieser Arbeit analysierten sozialen Medien und Messenger-Diensten sind in den meisten Fällen sehr umfangreich und, wie bereits weiter oben erwähnt, erfolgt die Einwilligung meist, ohne diese gelesen zu haben (Cakebread, 2017). Und selbst nach dem Lesen ist vielen Nutzer:innen nicht immer klar, wofür sie ihre Zustimmung erteilt haben. Im Folgenden werden nun die unter Punkt 1.4 genannten sozialen Medien und Messenger-Dienste hinsichtlich ihrer Datenschutzrichtlinien genauer betrachtet.

2.1.2.1 Meta Platforms Inc. (Facebook, Instagram)

Facebook

Das 2004 unter anderem von Mark Zuckerberg gegründete soziale Netzwerk Facebook gehört zu den erfolgreichsten Social-Media-

Plattformen überhaupt und konnte im vierten Quartal 2021 rund 2,91 Milliarden aktive Nutzer:innen weltweit verzeichnen (Statista Research Department, 2022). Zugleich steht das Unternehmen von Beginn an bezüglich seiner Datenschutzpraktiken und zahlreicher Verstöße gegen das Datenschutzrecht in der Kritik. Zu den größten und aktuellsten Skandalen zählt unter anderem der 2018 öffentlich gewordene Fall um Cambridge Analytica, bei dem die Daten von rund 87 Millionen Nutzer:innen abgezogen worden sein sollen (Dachwitz, Rudl & Rebiger, 2018). 2021 wurde bekannt, dass persönliche Daten von 530 Millionen Facebook-Mitgliedern im Internet veröffentlicht worden sein sollen (Verbraucherzentrale, 2021).

Trotz der öffentlichen Kritik und dem bekannten Geschäftsmodell, mit dem Sammeln und Verkaufen von (Nutzer:innen-)Daten ein Vermögen zu generieren, halten viele Nutzer:innen dem Netzwerk Facebook bzw. der Gesellschaft Meta Platforms Inc., die Treue. Das liegt unter anderem daran, dass der Wert vieler Daten und damit verbundene Risiken immer noch nicht bekannt zu sein scheinen.

Instagram

Das Soziale Netzwerk Instagram, dessen Schwerpunkt auf Video- und Foto-Sharing liegt, erschien erstmalig im Jahr 2010. Bereits zwei Jahre später, im Jahr 2012, wurde es von Facebook, mittlerweile Meta Platforms, übernommen (Meta Startseite, 2022).

Instagram teilt sich eine gemeinsame Datenschutzrichtlinie mit Facebook und stand aufgrunddessen ebenfalls schon häufiger in der Kritik. Erschwerend kommt hinzu, dass die Nutzung bereits ab 13 Jahren erlaubt ist (Meta Startseite, 2022). Kinder in diesem Alter sind meist nicht in der Lage, die Inhalte dieser Richtlinie sinnerfassend zu lesen und die Folgen des Daten-Teilens abzuschätzen.

Meta Platforms Inc.

Am 28. Oktober 2021 gab Facebook-Gründer Mark Zuckerberg bekannt, den bisherigen Mutterkonzern Facebook Inc. in Meta umzubenennen (Meta Tech at Meta, 2021). Soziale Medien wie Facebook und Instagram sowie der Messenger WhatsApp und weitere Dienste werden seither als Produkte von Meta bezeichnet. Die Datenschutzrichtlinien wurden dabei größtenteils zu einer gemeinsamen zusammengefasst (Anm. WhatsApp verfügt nach wie vor über eine eigene), die seit 1. Jänner 2023 gültig ist und nun mehr als 22.300 Wörter umfasst (Meta Datenschutzrichtlinie, 2023).

Neben dem Umfang hat sich auch die Transparenz zum Umgang mit den Daten nicht verbessert. Am 4. Jänner 2023 entschied der Europäische Datenschutzausschuss (EDSA), dass die Nutzung von personenbezogenen Daten von Nutzer:innen für personalisierte Werbung ohne eindeutige Einwilligung nicht im Einklang mit der DSGVO steht. Konkret geht es hierbei um eine Klausel in den Meta AGB, die es dem Konzern bisher ermöglichen soll, Nutzer:innen keine Option für oder gegen personalisierte Werbung anzubieten. Der österreichische Jurist und Datenschützer Max Schrems von der Plattform noyb (Non of your business) hat seit Einführung der DSGVO 2018 diesbezüglich mehrere Beschwerden eingereicht. Drei davon wurden nun entschieden. Neben einem generellen Stopp personalisierter Werbung in der EU hat die EDSA zusätzlich eine Geldstrafe von 390 Millionen Euro aufgrund der Datenschutzverstöße über Meta verhängt (noyb, 2023).

2.1.2.2 Twitter

Der Mikroblogging-Dienst Twitter wurde 2006 von Jack Dorsey, Biz Stone und Evan Williams in San Francisco zunächst unter dem Namen

„twtr“ gegründet und 2007 dann in Twitter unbenannt. Zunächst war das Zeichenlimit auf 140 Zeichen beschränkt und wurde 2016 auf 280 Zeichen ausgeweitet. Der Schwerpunkt der Kommunikationsplattform liegt in der Verbreitung von Kurznachrichten und Kommentaren – Tweets genannt. Im Gegensatz zu anderen sozialen Medien wie Facebook steht nicht die Vernetzung mit anderen Nutzer:innen im Vordergrund (Wikipedia - Twitter, 2023).

Eine weitere Besonderheit besteht in der häufigen Verwendung von sogenannten Hashtags (#hashtag). Damit versehen machen Schlagwörter einzelne Inhalte leichter auffindbar und diese zum Teil auch populärer, je öfter sie verwendet werden. Inzwischen hat sich der Hashtag auch in anderen sozialen Medien etabliert (Wikipedia - Hashtag, 2023). Neben Privatpersonen, Organisationen und Unternehmen wird der Mikroblogging-Dienst häufig von Journalist:innen verwendet.

Im Oktober 2022 wurde Twitter Inc. von Tesla-Gründer Elon Musk für 44 Milliarden US-Dollar gekauft. Bereits im Vorfeld wurde die Übernahme stark kritisiert, da eine Zunahme von Hassreden und Desinformationen befürchtet wurde (Tagesschau, 2022). Aber auch die Technologie von Twitter hinsichtlich des Schutzes von Nutzer:innendaten steht immer wieder in der Kritik. Peiter Zatko, IT-Experte und ehemaliger Sicherheitschef bei Twitter, spricht von zahlreichen Sicherheitsmängeln und veralteten Standards bezüglich IT-Sicherheit (Süddeutsche Zeitung, 2022).

Dass diese Kritik berechtigt sein könnte, zeigt ein Ende 2022 bestätigtes Datenleck. Profildaten inklusive Mailadressen und Telefonnummern von über 200 Millionen Twitter-Nutzer:innen befinden sich inzwischen kostenlos im Netz (Der Standard, 2023). Für Betroffene stellt das ein hohes Sicherheitsrisiko dar, da Cyberkriminelle diese Daten unter anderem für die Verbreitung von Phishing-Mails verwenden können. Dabei handelt es sich um E-Mails,

die Cyberkriminelle zum Teil in großem Stil mit dem Ziel versenden, Passwörter und weitere persönliche Daten von Nutzer:innen zu erschleichen und/oder Schadsoftware (sogenannte Malware) zu verbreiten, was mit hohen finanziellen Risiken, aber auch Imageschäden verbunden sein kann (Bundesamt für Sicherheit in der Informationstechnik, 2023).

2.1.2.3 TikTok

TikTok ist eine Plattform für das Erstellen und Teilen von Kurzvideos und einer der wenigen großen Unternehmen, deren Hauptsitz sich nicht in den USA, sondern in China befindet. Mit über 5300 Wörtern ist die Datenschutzrichtlinie sehr umfangreich (TikTok Datenschutzrichtlinie, 2022). Die Plattform wird schon seit längerer Zeit heftig für seine Daten- und Jugendschutzbestimmungen kritisiert (Köver, 2021). Beim Vergleich der Plattform-Richtlinien wird deutlich, dass TikTok noch wesentlich intransparenter mit den Nutzer:innendaten agiert, als das bei den amerikanischen Netzwerken der Fall ist. So findet sich beispielsweise in der gesamten Richtlinie kein Hinweis auf die besonders schützenswerten Daten aus Artikel 9 der Datenschutzgrundverordnung und das, obwohl eine Vielzahl davon gesammelt und verarbeitet werden (TikTok Datenschutzrichtlinie, 2022). Einige der Formulierungen sind inhaltlich kritisch zu betrachten, wie ein Auszug in Abbildung 1 unten zeigt. Hier wird Nutzer:innen suggeriert, dass das Sammeln dieser Daten ihre Sicherheit und


ihr Wohlergehen gewährleisten würde. Genau genommen lässt sich aus dieser Formulierung die Rechtfertigung für weitere Datenerhebungen ableiten und könnte somit als Irreführung bezeichnet werden.

2.1.2.4 LinkedIn

LinkedIn ist ein soziales Netzwerk, das für die Pflege von Geschäftskontakten und zur Knüpfung geschäftlicher und beruflicher Verbindungen konzipiert wurde. Der Sitz des 2002 gegründeten Unternehmens liegt in den USA, 2016 wurde es von Microsoft übernommen. Laut eigenen Angaben sind über 774 Millionen Nutzer:innen aus mehr als 200 Ländern auf der beruflichen Plattform aktiv (LinkedIn Startseite, 2022).

Die Datenschutzrichtlinie des Unternehmens umfasst über 6600 Wörter und ist somit äußerst umfangreich. Im Gegensatz zu anderen sozialen Netzwerken sind allerdings nur wenige personenbezogene Angaben (Name und Kontaktdaten) verpflichtend, um den Dienst nutzen zu können. Möchten Nutzer:innen allerdings vom vollen Funktionsumfang profitieren, sind weitere Angaben wie beispielsweise Ausbildung und Abschlüsse, Arbeitserfahrung mit Nennung der jeweiligen Unternehmen sowie Kenntnisse und Fähigkeiten zu machen (LinkedIn Datenschutzrichtlinie, 2022). Neben der freien Nutzung gibt es auch die Möglichkeit einer kostenpflichtigen Premium-Mitgliedschaft.

- Wir verwenden Ihre Daten, um Ihre Sicherheit und Ihr Wohlergehen zu gewährleisten, unter anderem durch die Überprüfung von **Benutzerinhalten** (und, falls nach geltendem Recht zulässig, von Direktnachrichten und zugehörigen Metadaten) auf Verstöße gegen unsere **Nutzungsbedingungen, Richtlinien und andere Bestimmungen**. Wir schließen auch auf Ihr Alter und können Sie unter bestimmten Umständen bitten, zusätzliche Daten zur Bestätigung Ihres Alters anzugeben.



Ähnlich wie andere soziale Netzwerke hat auch LinkedIn mit einem erheblichen Datenschutzproblem zu kämpfen. Im Jahr 2021 wurden im Darknet private Daten von über 700 Millionen Nutzer:innen zum Verkauf angeboten. Darunter waren Angaben zu Mailadressen, Namen, Telefonnummer sowie Anschriften. Nachdem das Netzwerk schon 2016 Opfer eines Cyberangriffs geworden ist, dürfte ein Großteil der Daten aus dieser Zeit stammen (FAZ, 2021).

2.1.2.5 WhatsApp

Der Instant-Messaging-Dienst WhatsApp wurde 2009 in den USA gegründet und gehört seit 2014 zu Facebook Inc. (WhatsApp Datenschutzrichtlinie, 2022). Nach der Umbenennung des Mutterkonzerns von Facebook Inc. zu Meta Platforms Inc. verfügt WhatsApp im Vergleich zu Facebook und Instagram weiterhin über eine eigene Datenschutzrichtlinie, die mit gut 10.800 Wörtern sehr umfangreich und in Bezug auf Datenschutz und Sicherheit nicht sehr transparent ist. Nachdem die Verantwortlichen 2021 bekannt machten, dass die Nutzungsbedingungen des Dienstes geändert werden sollten und Daten nun offiziell an Facebook weitergeleitet werden dürften, hat WhatsApp durch den medialen Diskurs innerhalb kurzer Zeit zahlreiche Nutzer:innen an die Konkurrenz verloren (Zeit Online, 2021). Neben dem Status, der Telefonnummer, dem Profilbild und Geburtsdatum erhält WhatsApp durch die Anmeldung auch Zugriff auf das persönliche Telefonbuch der Nutzer:innen. In der Datenschutzrichtlinie wird zudem an mehreren Stellen betont, was der Dienst nicht sammeln kann oder weiterleitet, wobei diese

Angaben zum Teil irreführend sind, wie das Beispiel in Abbildung 2 verdeutlicht. So steht dort zu Beginn, dass die Kontakte nicht mit Facebook geteilt werden. Im letzten Satz heißt es dann, dass die Kontaktlisten nicht mit anderen Apps von Facebook geteilt werden. Das wirft die Frage auf, ob nun die Kontakte oder Kontaktlisten nicht mit Facebook oder deren Apps geteilt werden. Formulierungen wie diese tragen keineswegs zum besseren Verständnis der Richtlinie bei.

2.1.2.6 Signal

Signal ist ein 2013 gegründeter Messenger-Dienst der gemeinnützigen Signal-Stiftung. Im Gegensatz zu anderen Diensten zeichnet sich dieser durch eine hohe Datensparsamkeit und eine kurze Datenschutzrichtlinie mit ca. 500 Wörtern aus. Für die Installation muss lediglich die Tel.-Nummer von Nutzer:innen registriert werden. Diese macht eine Person allerdings eindeutig identifizierbar. Durch die sogenannte Ende-zu-Ende-Verschlüsselung ist es nicht möglich, auf die Inhalte von Nachrichten zuzugreifen. Allerdings muss beachtet werden, dass sich die Server des Dienstes in den USA befinden und eine Durchsetzung der DSGVO mangels Kooperation der lokal zuständigen Behörden scheitert. Dies gilt im Umkehrschluss nicht für die Interessen der US-amerikanischen Behörden, die sich im Zweifelsfall vorbehalten, dass ihnen der Zugriff auf Daten wie Telefonnummern und Name gewährt werden muss. Positiv zu erwähnen ist, dass der Quellcode des Dienstes Open-Source und somit für jede:n einsehbar ist, wodurch ein Datensammeln im Geheimen nicht möglich ist (Signal Datenschutzrichtlinie, 2022).

Wir teilen deine Kontakte nicht mit Facebook: Wenn du uns die entsprechende Berechtigung erteilst, greifen wir nur auf die Telefonnummern in deinem Adressbuch zu, um einen schnellen und zuverlässigen Nachrichtenaustausch zu ermöglichen. Wir teilen deine Kontaktliste nicht mit anderen Apps von Facebook.

2.2 Informationswahrnehmung und Interpretation

Die Quantität der Inhalte der in dieser Arbeit untersuchten Datenschutzrichtlinien erschwert es Nutzer:innen für sie relevante Informationen zu erfassen und richtig einzuordnen. In erster Linie geht es also um die Erhöhung deren Sichtbarkeit. Die Wahrnehmung von Informationen bildet die Grundlage für das Verstehen selbiger und macht sie somit für die Nutzer:innen zugänglich. Die Sichtbarmachung der einzelnen Daten allein führt allerdings noch nicht unbedingt zum generellen Verständnis, da deren Bedeutungen und Abhängigkeiten untereinander nicht ersichtlich sind. Die Lösung des Problems liegt also nicht in der reinen Reduktion der Inhalte, sondern vor allem an der anschließenden Aufbereitung.

Im ersten Teil dieses Kapitels soll beleuchtet werden, welche Fähigkeiten bei der Informationswahrnehmung im Allgemeinen sowie in Bezug auf Bilder eine Rolle spielen. Dieser Abschnitt bezieht sich vor allem auf die Theorien der Psychologen James J. Gibson in *Wahrnehmung und Umwelt* sowie John M. Kennedy in *Psychology of Picture Perception*.

Der zweite Unterpunkt widmet sich der Informationswahrnehmung von Text und Zeichen, deren Vermittlung und den erforderlichen Fähigkeiten beim Verstehen und der Interpretation selbiger. Des Weiteren beschäftigt sich dieser Abschnitt mit der Semiologie (auch Semiotik), also der Lehre von sprachlichen und außersprachlichen Zeichen und bezieht sich hier vor allem auf die Theorien des Genfer Sprachwissenschaftlers Ferdinand de Saussure (1857-1913).

Im letzten Abschnitt dieses Kapitels liegt der Fokus auf den Möglichkeiten der Simplifizierung von Texten, also wie die Datenschutzrichtlinien der unter Punkt 1.4.2 angeführten


Plattformen und Diensten durch Visualisierungen und der Übertragung in ein Zeichensystem zugänglicher gemacht werden können. Dies basiert vordergründig auf den Theorien des französischen Kartographen Jacques Bertin sowie des US-amerikanischen Designers John Maeda.

2.2.1 Wahrnehmung von Informationen

Wie Menschen ihre Umwelt im Allgemeinen wahrnehmen und darin enthaltene Informationen aufnehmen, ist ein Schwerpunkt verschiedener Disziplinen (unter anderem der Wahrnehmungspsychologie), aus denen zahlreiche Theorien abgeleitet wurden. Aufgrund des genannten Schwerpunkts beschränkt sich diese Arbeit auf die Thesen der (Wahrnehmungs-) Psychologen James J. Gibson und John M. Kennedy.

Für Ersteren ist die Wahrnehmung „[...] eine Leistung des Individuums, nicht eine Erscheinung auf der Bühne seines Bewußtseins [sic!]“ (Gibson, 1982, S. 257). Es handelt sich also um einen Umstand, der nicht ohne Weiteres passiert, sondern die Aufmerksamkeit der jeweiligen Person erfordert. Gibson beschreibt den Akt der Informationsaufnahme des Weiteren als „[...] eine Aktivität, die nie aufhört und nicht abgebrochen wird“ (Gibson, 1982, S. 258). Individuen sind in ihrer Umwelt ständig Reizen ausgesetzt. Diese können chemischer, osmotischer, thermischer, mechanischer, akustischer sowie optischer Natur sein (Spektrum.de, 1999).

Für die vorliegende Arbeit sind vornehmlich die optischen Reize, die eine visuelle Wahrnehmung ermöglichen, von Bedeutung. In einem Zeitalter, das von digitalen Kommunikations- und Informationstechnologien geprägt ist und sich ständig weiterentwickelt,



sind es vor allem Bilder unterschiedlichster Art, die bei der visuellen Informationswahrnehmung und -aufnahme eine tragende Rolle spielen. Bilder wie Worte sind Träger von Informationen, senden diese aus, befördern sie (Gibson, 1982, S. 261). Die Ästhetik spielt dabei zunächst eine untergeordnete Rolle. Für John M. Kennedy ist die künstlerische Umsetzung oder Beschaffenheit eines Bildes unabhängig von der Frage, ob dieses informativ sein kann. Bilder, die Informationen bereitstellen sollen, sind seiner Ansicht nach ein Mittel der Kommunikation, des Zeigens und Betrachtens (Kennedy, 1974, S. 3-4).

In Bezug auf die in dieser Arbeit behandelten Datenschutzrichtlinien geht es vor allem um das Zeigen bzw. Aufzeigen der darin enthaltenen Informationen durch Icons. Um diese wahrzunehmen und das Dargestellte richtig ‚lesen‘ und interpretieren zu können, ist es notwendig, auf bereits existierendes explizites Wissen zurückgreifen zu können, was zu späteren Zeitpunkt noch genauer erläutert wird.

Allerdings verweist auch Kennedy im weitesten Sinn auf eine Art ‚Vorwissen‘ und zwar dahingehend, dass Bilder konventionell und durch starke, teils willkürliche Kanons an die Kultur gebunden sind, die sie hervorbringt (Kennedy, 1974, S. 48). Somit gilt es zu beachten, dass die in dieser Arbeit entwickelten Icons ihre Funktion der Informationsvermittlung auch nur beschränkt erfüllen können, da die kulturelle Prägung, auch durch Sprache und Schrift, einen großen Einfluss auf die Wahrnehmung und Interpretation nimmt.

Studien, beispielsweise aus dem Bereich der kognitiven Psychologie, belegen aber dennoch, dass Informationen aus Bildern anders verarbeitet werden als sprachliche und im Vergleich leichter erinnert werden können (Anderson, 1988, S. 80 ff.). Diese These vertritt auch Gibson, indem er anmerkt, dass es sich aus Bildern „[...] mit weniger Anstrengung lernen

[lässt] als aus Worten“ (Gibson, 1982, S. 283). Basierend auf diesen Ansätzen erfolgt im späteren Teil dieser Arbeit die Konzeption des informationsgrafischen Zeichensystems in Form von Icons, die relevante Inhalte der Datenschutzrichtlinien von sozialen Medien für Rezipient:innen zugänglicher machen sollen. Im nächsten Abschnitt wird dafür aber zunächst ein weiterer Bereich der Wahrnehmung und der Vermittlung von Informationen beleuchtet – und zwar durch Zeichen.

2.2.2 Wahrnehmung und Vermittlung durch Zeichen

Was genau ein Zeichen ist, darüber gibt es in der Geschichte der Semiotik zahlreiche Modelle und Definitionen. Eine mittelalterliche Definition beschreibt ein Zeichen recht allgemein als *aliquid stat pro aliquo*, also als „etwas, das für etwas anderes steht“ (Nöth, 2000, S. 137).

Der Grafikerdesigner und Gestalter Otl Aicher und der Kommunikationswissenschaftler Martin Krampen beschreiben im Buch *Zeichensysteme der visuellen Kommunikation* die Welt als Zeichenwelt, in der „Bilder, Worte, Symbole, Sätze aber auch Handlungen, Äußerungen, Gesten und Blicke [können] als Zeichen verstanden werden“ können (Aicher & Krampen, 1996, S. 5). Zeichensysteme sind ein Mittel der Kommunikation, der Verständigung in der Gesellschaft. Bildsymbole haben im Vergleich zur gesprochenen und geschriebenen Sprache den Vorteil, Sprachbarrieren teilweise überwinden zu können (Aicher & Krampen, 1996, S. 5). Wie diese Informationen von Rezipient:innen wahrgenommen und interpretiert werden, hängt allerdings von ihrem Vorwissen und kulturellen Hintergrund ab.

Der Philosoph Ludwig Wittgenstein formulierte dies folgendermaßen: „Was jedes Bild, welcher Form immer, mit der Wirklichkeit gemein

haben muss, um sie überhaupt – richtig oder falsch – abbilden zu können, ist die logische Form, das ist die Form der Wirklichkeit“ (Wittgenstein, 1922). Das heißt, das dargestellte Zeichen muss für Betrachter:innen mit etwas ihnen Bekannten verknüpft werden können. Ein einfaches Beispiel ist das Ampelsystem mit den Farben rot, gelb und grün. In diesen Breitengraden vor allem durch den Straßenverkehr bekannt, sind Rezipient:innen dennoch in der Lage, das System auch in anderen Zusammenhängen zu verstehen.

Ein aktuelleres Beispiel ist die sogenannte Corona-Ampel, die zur Risikoeinschätzung der Verbreitung von COVID-19 in Österreich eingesetzt wurde (Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz, 2020). Obwohl diese Ampel neben den Farben rot, gelb, grün auch orange enthielt, waren die damit verbundenen Informationen interpretierbar. Die Farbe Rot, die im Straßenverkehr für Halt steht, konnte in Bezug auf Corona gleichzeitig als hohes Risiko gedeutet werden. Das setzt allerdings voraus, dass diese Bedeutungen von Zeichen irgendwann erlernt worden sind. Ein Mensch, der abseits der modernen Gesellschaft aufwächst und sich nie mit dem Straßenverkehr auseinandersetzen muss, kann mit diesen Zeichen kein weiteres Wissen verknüpfen.

Ein anderes Beispiel ist das Schreiben und Lesen eines Satzes. Damit dies möglich ist, muss das Zeichensystem in der jeweiligen Sprache erlernt werden. Im ersten Schritt erfolgt dies durch das Erkennen der einzelnen Buchstaben. Der Schriftgestalter Adrian Frutiger beschreibt diesen Leseprozess am Beispiel von Kindern, die Wörter zu Beginn erst buchstabieren, bis sich das Unterbewusste nicht mehr auf Einzelbuchstaben konzentriert, sondern auf Silben und Wortbilder (Frutiger, 1998, S. 198). Das Erlernen dieser Buchstabenverbindungen bildet die Grundlage beim Lesen und Schreiben der jeweiligen Sprache.

Diese sprachlichen Zeichensysteme haben allerdings den Nachteil, begrenzt zu sein, d. h. sie sind auf die Nationalsprache beschränkt, was ein Verständnis im internationalen Rahmen verhindert.

Bilder und Bildzeichen haben deshalb in den vergangenen Jahrzehnten enorm an Bedeutung gewonnen (Krampen, Götte & Kneidl, 2007, S. 14). Sie überwinden die sprachliche Barriere, da sie von Rezipient:innen anders wahrgenommen werden. Krampen und Aicher zufolge erschließt „das Bilddenken [...] den Sinn vom Ganzen hin zum Einzelnen, das Schriftdenken von Einzelnen hin zum Ganzen“ (Aicher & Krampen, 1996, S. 100). Die sprachlichen Zeichen an sich sind arbiträr. Durch sie können Sachverhalte, Objekte usw. beschrieben werden. Hierbei gilt es zu beachten, dass der Ausdruck eines sprachlichen Zeichens – genauer gesagt, eines Substantives – nicht den Inhalt desselbigen erfordert.

Der deutsche Begriff *Baum* heißt im Englischen *tree* – zwei verschiedene Wörter im Ausdruck, die inhaltlich aber dasselbe beschreiben. Nach Sprachwissenschaftler Ferdinand de Saussure verfügt das sprachliche Zeichen über eine dyadische Struktur, wobei er die Ausdruckseite, also das Lautbild, als Signifikanten, die inhaltliche Seite, also die Vorstellung eines Zeichens, als Signifikat bezeichnet (siehe Abb. 3, S. 28). Die Zusammensetzung dieser beiden Teile ergibt seiner Theorie nach das Zeichen [signe] (Nöth, 2000, S. 74). An dieser Stelle ist anzumerken, dass sich Saussure ausdrücklich auf sprachliche Zeichen bezieht. Dennoch wird die Theorie auch auf andere Zeichenarten angewendet (Nöth, 2000, S. 73.). Das ist insofern sinnvoll, als dass außersprachliche Zeichen von Rezipient:innen meist mit einem sprachlichen verknüpft bzw. in Verbindung gebracht werden. Weitere Begriffsdefinitionen zur Semiotik erfolgen unter Punkt 2.3.1.

Allerdings gilt es hier noch anzumerken, dass einzelne Zeichen oder Bilder Worte nicht einfach ersetzen können. Für den Medienwissenschaftler Frank Hartmann und Grafikdesigner Erwin Bauer steht ein Zeichen „nicht an sich für sein Objekt, sondern immer nur im Bezug auf einen Interpreten“ (Hartmann & Bauer, 2006, S. 40). Eine absolute Eindeutigkeit eines Zeichens wäre ihrer Ansicht nach nur möglich, wenn alle Menschen gleich denken und dem zufolge über dasselbe Wissen verfügen würden (Hartmann & Bauer, 2006, S. 40). Dieser Sachverhalt wurde bereits unter Punkt 2.2.1 zum Thema der kulturellen Bindung von Zeichen dargestellt.

Ein vollständiger Ersatz von Sprache bzw. Worten durch Zeichen ist nicht Ziel dieser Arbeit. Vielmehr geht es um die visuelle Simplifizierung einzelner Inhalte in den Datenschutzrichtlinien, unter anderem durch die Reduktion der Texte – näheres dazu unter folgendem Punkt. Die dafür entwickelten Icons sollen den Transport der relevanten Informationen vordergründig unterstützen, die Wahrnehmung erleichtern und beschleunigen.

2.2.3 Simplifizierung durch Textvisualisierung

Die Informationsvisualisierung oder genauer gesagt die Textvisualisierung kann wesentlich dazu beitragen, eine Vielzahl an Informationen zu veranschaulichen. Der Visualisierungsspezialist Andy Kirk sieht die Notwendigkeit darin, Nutzer:innen durch verschiedene Darstellungsformen von Informationen möglichst weitgehend bei deren Verständnis, also dem inhaltlichen Begreifen, zu unterstützen und die Bedeutung der Daten bzw. Informationen zu finden. Dadurch können seiner Ansicht nach unter anderem vorhandenes Wissen aktiviert oder ganz neue Themen nähergebracht werden (Kirk, 2016, S. 77ff.).

Das inhaltliche Begreifen von Informationen wird auch bei Jacques Bertin aufgegriffen, der davon ausgeht, dass eine grafische Darstellung so beschaffen sein sollte, dass sie ein im Gedächtnis speicherbares grafisches Bild schafft (Bertin, 1974, S. 170). Für die Übertragung der Informationen aus den Datenschutzrichtlinien bedeutet dies im ersten Schritt,

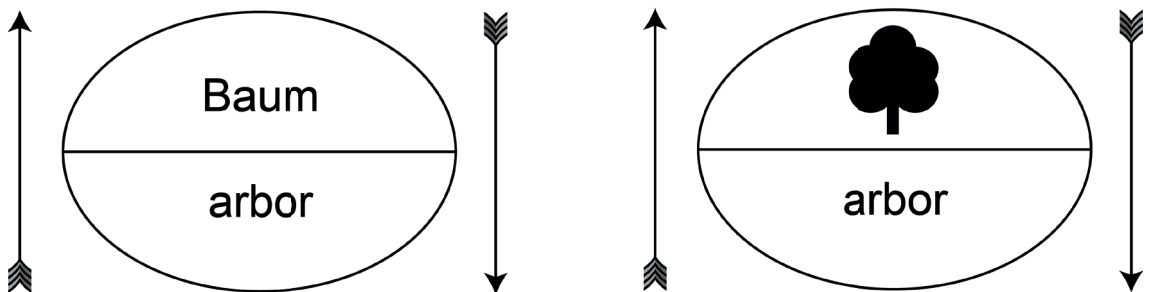


Abb. 3: Saussures Model des sprachlichen Zeichens und die Vorstellung des Bildes
Quelle: Nöth, 2000, S. 74

geeignete Zeichen zu entwickeln, die ein rasches Verständnis bei den Nutzer:innen möglich machen. Bertin hat diesen Umstand sehr treffend formuliert: „Eine graphische Information verstehen heißt, visuell ein graphisches Bild oder mehrere graphische Bilder im Gedächtnis zu speichern“ (Bertin, 1974, S. 168).

Die Voraussetzung für eine Speicherung bilden ihm zufolge drei Funktionen – die Registrierung, Vermittlung und Weiterverarbeitung der Information (Bertin, 1974, S. 168-178). Die Registrierung dient einer Bestandsaufnahme und entspricht somit der Informationswahrnehmung. Die Vermittlung erfordert, dass das außersprachliche Zeichen sich im Gedächtnis speichern lässt (Bertin, 1974, S. 170). Das setzt voraus, dass es nicht zu komplex gestaltet und – im bestmöglichen Fall – mit Bekanntem (Vorwissen) verknüpfbar ist. Die Weiterverarbeitung dient der Kategorisierung – also der eigentlichen Verknüpfung – mit bereits im Gedächtnis vorhandener Information, was zudem zu einer Vereinfachung führt. Das Zeichen wird dadurch verständlich und ist somit speicherbar (Bertin, 1974, S. 174).

Für die Simplifizierung der Informationen aus den Datenschutzrichtlinien ist es deshalb nicht zielführend, ein willkürliches Symbol zu entwickeln, das beispielsweise darstellen soll, dass die Plattform biometrische Daten verarbeitet. Da das Symbol den Nutzer:innen bis dahin nicht bekannt ist, werden sie die enthaltene Information folglich nicht verstehen. Ein längerer Textabschnitt, der diese Daten ausführlich erklärt, ist ebenfalls nicht dienlich. Bei der Entwicklung des Zeichensystems ist demnach darauf zu achten, auf vorhandenes Wissen der Nutzer:innen zurückzugreifen.

Da die Datenschutzrichtlinien der sozialen Medien sowohl im Umfang als auch in sprachlicher Hinsicht meist sehr komplex sind, ist es schwierig, inhaltliche Informationen zu erfassen.


In diesem Zusammenhang formuliert der US-amerikanische Informationswissenschaftler und Grafikdesigner Edward Tufte, dass die Menge der Details von der Schwierigkeit des Lesens zu unterscheiden sei, da diese ‚Unordnung‘ und ‚Verwirrung‘ als Designfehler zu betrachten und keine Wesensmerkmale der Information sind (Tufte, 1990, S. 51).

Diesbezüglich ist der Ansatz des Designers John Maeda in seinem Werk *The Laws of Simplicity* förderlich. „The simplest way to achieve simplicity is through thoughtful reduction“ (Maeda, 2006, S. 1). Eine überlegte Reduktion, also bewusstes Weglassen von Informationen, führt demnach zur Vereinfachung und macht die Inhalte zugänglicher. Wie bereits in der 1. Unterforschungsfrage formuliert, ist darauf zu achten, dass diese Reduktion nicht zu einer Verzerrung oder Verfälschung führt. Maeda schlägt deshalb folgende Fragestellungen vor:

HOW SIMPLE		HOW COMPLEX
	<--->	
YOU MAKE IT?		IT HAVE TO BE?

(Maeda, 2006, S. 1)

Wie bereits am Beginn dieser Arbeit erwähnt, ist die Komplexität der Datenschutzrichtlinien vor allem den gesetzlichen Vorgaben geschuldet. Das Vorhandensein eines umfangreichen Dokuments ist also notwendig. Gleichzeitig gibt es keine Gesetze oder Richtlinien, die es den Plattform-Betreibern untersagen würden, Nutzer:innen zusätzlich eine ‚Kurzfassung‘ bzw. einen Überblick zu den für sie relevanten Daten und deren Verarbeitungen zur Verfügung zu stellen. Basierend auf Maedas Fragestellungen sollte diese ‚nutzer:innenzentrierte Zusammenfassung‘ so einfach wie möglich gehalten werden. Das heißt, wo möglich, durch den Einsatz geeigneter, also leicht zu



lesender ‚Zeichen‘ (Icons) und einer klaren, verständlichen Sprache, ohne juristischer Verklausulierungen und ständigen Wiederholungen der verarbeiteten Datensätze und deren Zweck. Nach Hartmann und Bauer verlangt eine „Fülle an Information [verlangt] nach Reduktion der visuellen Sprache“ (Hartmann & Bauer, 2006, S. 113). Damit einhergehend bestünde, wie bereits weiter oben erwähnt, ein hoher Bedarf an „neutraler, klarer und einfach verständlicher visueller Sprache“ (Hartmann & Bauer, 2006, S. 113).

Auf diesen Empfehlungen und Theorien basierend erfolgt unter Punkt 3 das methodische Vorgehen und die Analyse der Datenschutzrichtlinien sowie – in weiterer Folge – die Entwicklung des Zeichensystems.

2.3 Konzeption eines informationsgrafischen Zeichensystems

Das Ziel der Masterarbeit ist, Nutzer:innen anhand eines informationsgrafischen Zeichensystems zu befähigen, sich rasch einen Überblick über die Inhalte der unter Punkt 2.1.2 angeführten Social-Media-Datenschutzrichtlinien zu verschaffen. Die entwickelten Zeichen, genauer gesagt Icons, werden anhand der Ergebnisse aus verschiedenen Nutzer:innen-Befragungen und Testings entworfen und fließen in den unter Punkt 2.4 beschriebenen Webseiten-Prototypen mit ein.

An dieser Stelle ist es notwendig, das Konzept der Semiotik, also der Zeichentheorie, genauer zu beleuchten. Des Weiteren werden einzelne Begriffe wie Symbol, Index, Icon und Piktogramm genauer definiert. Unter Punkt 2.3.2 erfolgt die Beschreibung des Konzepts, das dem für diese Arbeit entwickelten Zeichensystems zugrunde liegt.

2.3.1 Konzept der Semiotik: Begriffsdefinition und Abgrenzung

Die Semiotik ist per definitionem die Lehre bzw. Wissenschaft von Zeichen. Aus etymologischer Sicht ist der Begriff der Semiotik mit den griechischen Wörtern ‚Zeichen‘ und ‚Signal‘ verwandt (Nöth, 2000, S. 1). Wie bereits weiter oben erwähnt, gilt der Sprachwissenschaftler Ferdinand de Saussure als Begründer der modernen Semiotik. Dies betrifft allerdings vorrangig die Linguistik. Die allgemeine Zeichentheorie betreffend, insbesondere die nichtsprachlichen Zeichen, wird sein Einfluss geringer eingeschätzt (Nöth, 2000, S. 77).

Als eigentlicher Begründer der neueren Allgemeinen Semiotik gilt der Philosoph Charles Sanders Peirce (1839-1914). Im Gegensatz zu Saussure konzentriert sich seine Forschung der Semiotik nicht auf Linguistik, sondern orientiert sich an der Logik und Erkenntnistheorie (Nöth, 2000, S. 59). Die Semiotik von Peirce stützt sich auf drei Universalkategorien: Qualität, Relation und Repräsentation. Zeichen definiert er als Phänomene bzw. Phanerons der dritten Kategorie, also der Repräsentation. Die Phänomene der ersten und zweiten Kategorie können seiner Ansicht nach ebenfalls über zumindest semiotische Aspekte verfügen. In Bezug auf die menschliche Wahrnehmung nennt er drei weitere Universalkategorien, die seine Phänomenologie definieren: Erstheit, Zweitheit und Drittheit. Diese drei Elemente lassen sich mittels aufmerksamer Wahrnehmung in einzelnen Phänomenen erkennen (Nöth, 2000, S. 61). Die Kategorien definiert er folgendermaßen: Die Erstheit verbindet er unter anderem mit einem unreflektierten Gefühl, Freiheit, einer noch undifferenzierten Qualität.

Die Zweitheit ist die Kategorie der Bezugnah-

me, Reaktion, Realität und steht in Relation mit der ersten Kategorie. Im Gegensatz zur letzteren steht die zweite Kategorie für die Welt des Faktischen, zu etwas Entgegengesetztem. Die Drittheit schafft einen Bezug zu etwas Zweitem und ist somit die Kategorie der Vermittlung, Erinnerung, Kommunikation, Repräsentation und der Zeichen. Dieser Definition nach gehören Zeichen also in die Kategorie der Drittheit (Nöth, 2000, S. 61).

Als ein Phänomen der Drittheit der Piercischen Semiotik gilt, dass das Zeichen drei Korrelate in eine triadische Beziehung bringt. Das Zeichen (Repräsentant), das Objekt, auf das sich ersteres bezieht sowie die Bedeutung des Zeichens (Interpretant). Das Zeichen an sich steht für etwas oder jemanden, es repräsentiert ein Objekt. Aus dieser Relation entsteht das eigentliche Zeichen – der Interpretant. Ein Zeichen muss laut Peirce immer als solches interpretierbar sein. Als Beispiele nennt er unter anderem Wörter, Bilder, Signale, Bücher, aber auch Konzerte (Nöth, 2000, S. 62).

Obwohl die Semiotik von weiteren Persönlichkeiten geprägt und weiterentwickelt wurde, mit zum Teil sehr unterschiedlichen Richtungen und Schulen, liegt der Fokus dieser Arbeit – vor allem bezüglich der Entwicklung von Zeichen – hauptsächlich auf den beschriebenen

nen Theorien von Saussure und Peirce. Die Definitionen von letzterem sind im folgenden Punkt von besonderer Relevanz.

2.3.1.1 Definition Symbol, Index, Ikon, Piktogramm


Die Klassifikation der Zeichen von Peirce setzt sich aus drei Kategorien und Trichotomien zusammen (siehe Tabelle 1). Für diese Arbeit ist die zweite Trichotomie der Objektrelation relevant. Sie setzt sich aus den drei Klassen Ikon (Erstheit), Index (Zweitheit) sowie Symbol (Drittheit) zusammen. Im Folgenden werden die einzelnen Klassen genauer beschrieben.

Symbol

Der Begriff des Symbols wird in der Semiotik häufig mit dem des Zeichens gleichgesetzt, sollte aber eher als Unterklasse angesehen werden. In den wissenschaftlichen Disziplinen gibt es verschiedene Definitionen des Symbolbegriffs. Für Peirce sind es die Kriterien der Gesetzmäßigkeit und Gewohnheit, die zur Kategorie der Drittheit zählen, die ein Zeichen ausmachen. Arbitrarität und Konventionalität sind diesbezüglich zweitrangig und sind auch nicht die alleinigen Bedingungen, die ein Sprachzeichen zum Symbol machen. Für ihn

Kategorie / Trichotomie	I des Repräsentamens	II der Objektrelation	III des Interpretantenbezugs
Erstheit (Möglichkeit)	Qualizeichen	Ikon	Rhema
Zweitheit (Existenz)	Sinzeichen	Index	Dicent
Drittheit (Gesetz)	Legizeichen	Symbol	Argument

Tabelle 1: Peirce' neun Subzeichenklassen
Quelle: Nöth, 2000, S. 66



sind es eher die allgemeinen Regeln in der Sprachgemeinschaft, im gewissen Sinne einer Gesetzmäßigkeit folgend, die diese Symbolhaftigkeit bedingen. Ein Symbol wird zum Zeichen, indem es als solches verstanden und gebraucht wird (Nöth, 2000, 178-180).

Eine weitere Unterteilung des Symbols kann in die drei Arten des konventionellen, des ikonischen und des konnotativen Zeichens erfolgen (Nöth, 2000, S. 179-181).

Die Konventionalität wird bei Peirce, wie bereits weiter oben erwähnt, mit der Kategorie der Gewohnheit erweitert. Diese bedingt, dass es als Symbol interpretiert werden kann. Es ist substitutiv und als solches ein nicht-motiviertes Zeichen. Für Peirce grenzt es sich dadurch vom ikonischen (abbildenden) und indexikalischen (hinweisenden) Zeichen ab (Nöth, 2000, S. 179).

Das Symbol als ikonisches Zeichen setzt voraus, dass es mit seinem Objekt durch eine Beziehung verbunden ist, und zwar durch eine Form der Motivation, einer Ähnlichkeit oder Analogie. Für Saussure ist das Symbol ein motiviertes Zeichen, das nie gänzlich arbiträr ist. Auch in der Geschichte der Ästhetik, beispielsweise bei Kant und Hegel, wird der Begriff diskutiert. Letzterer definiert das Symbol, ähnlich wie Saussure, als ikonisch motivierte Zeichen mit einem Bedeutungsinhalt – was sie von arbiträren Zeichen unterscheidet (Nöth, 2000, S. 181).

Zu einem konnotativen Zeichen wird ein Symbol, wenn es neben einer primären noch über eine sekundäre Bedeutung verfügt (Nöth, 2000, S. 181-182). Konnotativ ist per definitionem „die assoziative, emotionale, stilistische, wertende [Neben]bedeutung eines sprachlichen Zeichens betreffend“ (Duden, online). Das Symbol verfügt demnach über einen Bedeutungsüberschuss. Bezogen auf die Semantik, also dem Inhalt und der Bedeutung der Symbole, ergeben sich daraus vier wei-

tere Richtungen, die hier zwar noch erwähnt, aber nicht genauer beschrieben werden: das Symbol als konkreten Ausdruck eines tieferen Sinnes, als Ausdruck von etwas Unergründbarem, als Irrationalität des Symbolischen sowie eines unbewussten Inhalts (Nöth, 2000, S. 182-183).

Index

Das indexikalische Zeichen wird in der Geschichte der Semiotik nach verschiedenen Kriterien klassifiziert. Für Peirce steht es im Gegensatz zum ikonischen und symbolischen Zeichen und gehört zur Zweitheit seiner Universalitätskategorien. Wie bereits weiter oben erwähnt, bedingt diese Zweitheit die unmittelbare Verbindung von einem Ersten mit einem Zweiten. Zeichen und Objekt stehen demnach in einer dyadischen Beziehung. Ein Index setzt voraus, dass es durch das Objekt, auf das es verweist, beeinflusst wird (Nöth, 2000, S. 186).

Ikon

Die Allgemeine Semiotik definiert ein Ikon als Zeichen, „welches das von ihm bezeichnete Objekt auf Grund einer Ähnlichkeitsbeziehung repräsentiert“ (Nöth, 2000, S. 193). Das heißt, dass zwischen Zeichenträger und dem zu bezeichnendem Objekt eine Similarität bestehen muss. Diese Ähnlichkeit ist der Peirscen Theorie nach allerdings sekundär, da sich das ikonische Zeichen aufgrund in ihm vereinender eigener Merkmale auf ein Objekt bezieht. Zudem unterscheidet er zwischen einem reinen Ikon und einem sogenannten Hypoikon, dem eigentlichen ikonischen Zeichen. Ersteres sieht er als Vorstufe des Letztgenannten (Nöth, 2000, S. 193).

Piktogramm

Piktogramme sind reduzierte und grafisch vereinfachte Darstellungen mit dem Ziel, Informationen zu vermitteln. Besonders häufig sind sie

dort vorzufinden, wo Menschen über Sprachgrenzen hinweg zu bestimmten Umständen informiert werden sollen. Das trifft beispielsweise auf Wegleitsysteme von Flughäfen, Bahnhöfen oder Krankenhäuser zu (Christian, 2017, S. 25-26).

Ein bekanntes Beispiel für die Relevanz der visuellen Kommunikation durch Piktogramme findet sich bei den olympischen Spielen 1972 in München. Otl Aicher und seine Mitarbeiter:innen haben diese eigens für diese Veranstaltung entwickelt und weltweit bekannt gemacht (Aicher & Krampen, 1996, S. 5). Piktogramme finden beispielsweise auch Verwendung als Verkehrszeichen (z. B. Ampelmännchen) oder als Gefahrensymbole und sind diesbezüglich genormt. Sie sind Projektionen und Abstraktionen der Wirklichkeit, auf das wesentliche reduziert und sollten einfach verständlich soweit möglich ohne zusätzlichen Text auskommen.

Nachteilig bei Piktogrammen (aber auch bei anderen Zeichensystemen) wird gesehen, dass deren Bedeutung erlernt werden oder sich auf ein Vorwissen von Rezipient:innen beziehen muss. Eine Unterscheidung zwischen Ikon und Piktogramm kann am ehesten in deren Verwendung gesehen werden. Piktogramme sind stark auf das Wesentliche reduziert und sehr häufig normiert, z. B. im Straßenverkehr, während Ikons aufwändiger und abstrakter dargestellt werden, beispielsweise in der IT oder zu Unterhaltungszwecken (Götz & Rigamonti, 2015, S. 84).

2.3.1.2 Ikonizitätsgrade

Die Eigenschaft der Ikonizität von Zeichen geht auf den US-amerikanischen Semiotiker und Philosophen Charles W. Morris (1901-1974) zurück. Demnach „ist ein Zeichen [...] in dem Maße ikonisch, in dem es selbst über die Eigenschaften seiner Denotate verfügt“

(Nöth, 2000, S. 197). Ein Denotat bezeichnet gemeinhin den „begriffliche[n] Inhalt eines sprachlichen Zeichens im Gegensatz zu den emotionalen Nebenbedeutungen“ (Dudenredaktion - Denotat, o.J.). Nach Morris trifft diese Bezeichnung allerdings auch auf außersprachliche Zeichen zu.

Peirce unterscheidet in der Ikonizität aufgrund des triadischen Kategoriesystems zwischen drei Modi, die durch Bilder, Diagramme und Metaphern repräsentiert werden können. Das Bild verfügt demnach über den höchsten Grad der Ikonizität, da diese durch einfache Qualitäten repräsentieren. Bei Diagrammen und Metaphern nimmt der Ikonizitätsgrad ab. Erstere hängen relationsbedingt von Indices und Symbolen ab, letztere beruhen auf der Ähnlichkeit von zwei symbolischen Zeichen (Nöth, 2000, S. 195-196). An dieser Stelle ist anzumerken, dass die unterschiedlichen Theorien der Ikonizität durchaus umstritten sind, weshalb eine gemeingültige Definition nicht möglich ist.

2.3.2 Entwicklung eines Zeichensystems

Eine Grundlage für die Entwicklung von Zeichen, genauer gesagt Icons, ist, dass diese von Nutzer:innen verstanden werden. Nach Otl und Krampen sollte demnach „die Häufigkeit eines Illustrationselementes statistisch signifikant [...] sein“ (Aicher & Krampen, 1996, S. 112). Das heißt, dass die in dieser Arbeit gestalteten Icons einem Usability-Testing unter Nutzer:innen unterzogen werden müssen, um feststellen zu können, welches Zeichen am ehesten mit dem damit verbundenen Inhalt in Beziehung gebracht werden kann. Im Folgenden soll das zu Grunde liegende Konzept für die Entwicklung genauer beschrieben werden.

2.3.2.1 Grundlagen und Überlegungen

Die Einwilligung in die Datenschutzrichtlinien erfolgt, wie bereits zu Beginn dieser Arbeit festgestellt, größtenteils ohne dass die Nutzer:innen diese gelesen haben. Neben dem großen Umfang von bis zu ca. 22.300 Wörtern (z. B. Meta Datenschutzrichtlinie, 2023) ist häufig auch der Inhalt der Richtlinien nur schwer zugänglich.

Die Idee ist also eine Plattform bereitzustellen, die es ermöglicht, wichtige Inhalte und Datenkategorien der hier untersuchten Medien und Dienste im ersten Schritt grafisch darzustellen. Das Ziel des Zeichensystems ist es, die verschiedenen Kategorien sichtbar zu machen und Nutzer:innen so einen niederschweligen Zugang zu diesen Schriftstücken zu ermöglichen. Neben interessierten Nutzer:innen kann die Plattform in einem weiteren Schritt auch für Schulungszwecke, beispielsweise zur Vermittlung von Medienkompetenz an Schulen, verwendet werden.

2.3.2.2 Übertragung von Kategorien in Zeichensystem

Im ersten Schritt ist es zunächst notwendig, geeignete Kategorien für Übertragung in ein Zeichensystem festzulegen. Die Europäische Datenschutzgrundverordnung gibt hier zwei grobe Blöcke zu den personenbezogenen Daten vor:

- allgemeine personenbezogene Daten nach Artikel 4,
- besondere Kategorien personenbezogener Daten gemäß Artikel 9 DSGVO

(EU Verordnung 2016/679, 2016)

Ersterer bezieht sich auf alle Informationen, anhand derer natürliche Personen identifiziert werden können bzw. bereits identifiziert

worden sind. Dazu gehören unter anderem: Name, Adresse, Telefonnummer, IP-Adresse, Profilbild, Geburtsdatum, Geo-Daten usw. Die besonderen Kategorien personenbezogener Daten nach Artikel 9 DSGVO sind hingegen genau definiert und in acht Punkte zusammengefasst:

- die rassische oder ethnische Herkunft
- politische Meinungen
- religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- genetische Daten
- biometrische Daten
- Gesundheitsdaten
- Sexualeben und sexuelle Orientierung

(EU Verordnung 2016/679, 2016)

Die Betreiber der sozialen Medien und Dienste sind dazu verpflichtet, diese Daten anzuführen, sofern diese von ihnen verarbeitet werden. Für die Erstellung eines Zeichensystems sind sie allerdings noch unzureichend bzw. können zum Teil auch zusammengefasst werden. Aus diesem Grund ist es notwendig, die Nutzer:innen in den Prozess der Kategorie-Bildung miteinzubeziehen, was unter Punkt 3.0 anhand verschiedener Methoden erfolgt.

2.3.2.3 Konzept Icon-Design

Ikons sind zu einem wichtigen Bestandteil des täglichen Lebens geworden. Sie vermitteln nonverbal Informationen, erklären Funktionen und Anwendungen. Damit diese visuelle Vermittlung gelingt, müssen Icons über bestimmte Funktionen verfügen. So muss der Sinn der Grafik für Nutzer:innen erkennbar sein. Ein zweiter Faktor ist die Vertrautheit – d.h., sie müssen für Nutzer:innen mit etwas Bekanntem, einem Begriff oder Objekt, verknüpfbar sein. Bei der visuellen Komplexität von Icons ist darauf zu achten, wie hoch die Anzahl der

einzelnen Elemente, beispielsweise horizontale und vertikale Linien, ist. Ist die Grafik zu komplex, hat dies wiederum Auswirkungen auf die Erkennbarkeit und Vertrautheit. Ein vierter Faktor ist der ästhetische Anreiz, den der Icon auf Nutzer:innen ausübt (Collaud, Reppa, Défayes, McDougall, Henchoz, Sonderegger, 2022). Letzterer ist für die Vermittlung der Information vernachlässigbar, da die Ästhetik, also ob eine Grafik als ansprechend oder nicht empfunden wird, sehr stark von der subjektiven Empfindung der Nutzer:innen abhängig ist.

Für die Entwicklung des Zeichensystems sind also die Faktoren der Sinnerfassung und Vertrautheit relevant. Zudem sollten die Icons nicht zu komplex gestaltet sein, also orientiert an John Maedas Fragestellungen: „How simple you make it? How complex does it have to be?“ (Maeda, 2006, S. 1).

2.4 Prototyp Click-Dummy: I AGREE to what I see

Der Prototyp wird als einfacher Click-Dummy einer Webseite in Figma entwickelt, einer browserbasierten Anwendung für einfaches Oberflächendesign während des Entwicklungsprozesses. Im weiteren Verlauf werden der Aufbau und Inhalt sowie angedachte Funktionen beschrieben. An dieser Stelle ist anzumerken, dass der finale Click-Dummy noch nicht über alle angedachten Anforderungen und Inhalte verfügt, sondern lediglich einen groben Überblick bieten und die Ausführung der angedachten Aufgaben für das Usability-Testing unter Punkt 3.5 ermöglicht.

2.4.1 Aufbau und Inhalt

Das Design der Startseite ist an die Idee eines Panopticons angelehnt, das von dem britischen Philosophen Jeremy Bentham als Konzept zum Gefängnisbau entworfen wurde.

Dabei handelt es sich um ein kreisförmig angelegtes Gebäude, wobei es von einem Punkt aus möglich ist, in alle Räume einzusehen (Bentham, J., 1791, S. 6-7).

Die Nutzer:innen des Prototypens schlüpfen hierbei in die Rolle der „Aufseher:innen“. Über den Button *Meine Netzwerke* werden in einem Halbkreis sämtliche von ihnen verwendete soziale Medien und Messenger Dienste angezeigt. Die Einrichtungsmöglichkeit dieser Funktion ist im Prototypen nicht enthalten. Dieser Aufbau symbolisiert, dass Nutzer:innen alle Daten sehen können, die von ihnen gesammelt werden.

Durch einen Klick auf die jeweilige Plattform gelangen die Nutzer:innen auf eine Detailseite, in der die jeweils gesammelten Daten in Form von Icons mit Kurzbeschreibung dargestellt sind. Mit einem weiteren Klick auf die Datenkategorie, z. B. *Gesundheitsdaten*, gelangen sie auf die Detailseite, wo eine genaue Beschreibung inklusive damit verbundener Risiken erfolgt.

In der Menüleiste erhalten Nutzer:innen Hintergrundinformationen zur EU-Datenschutzgrundverordnung, dem Datenschutzgesetz sowie weitere Informationen über die Risiken des Daten-Teilens. In einem anderen Menüpunkt finden sich Details zu den einzelnen sozialen Medien sowie die aktuellen Datenschutzrichtlinien. Dort könnte angedacht werden, die kritischen Passagen hervorzuheben, sodass Nutzer:innen beispielsweise direkt auf die Seite gelangen, auf der besonders schützenswerten Daten erwähnt werden. Zudem bietet es sich an, Nutzer:innen über Einschränkungsmöglichkeiten des Datensammelns auf der jeweiligen Plattform zu informieren.

Des Weiteren ist ein Menü-Punkt *News-Blog* angedacht, auf dem regelmäßig über beispielsweise Urteile zum Datenschutz, damit verbundene Strafen usw. informiert wird.

2.4.2 Entwürfe und Skizzierungen

Im Folgenden sind einige Vorabentwürfe und Ideen für den Prototypen – teilweise als Paper-Prototyp – abgebildet.

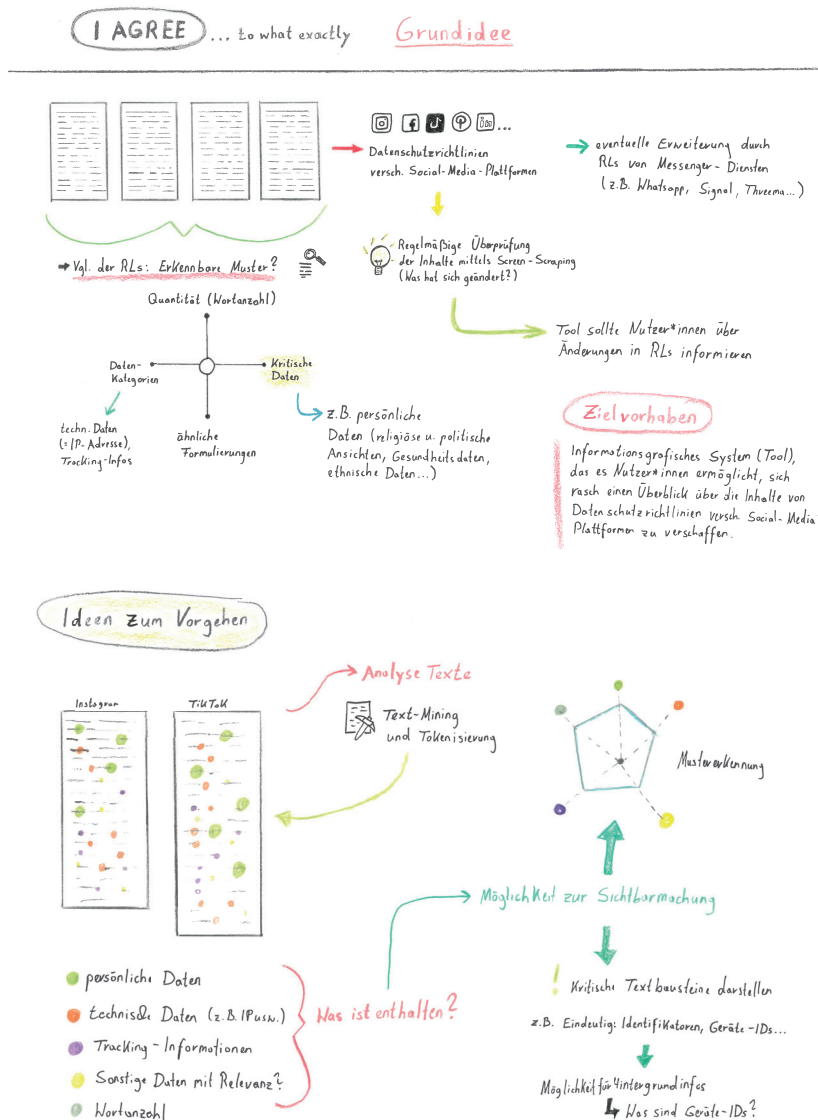


Abb. 4 und Abb. 5: Skizze Grundidee und Vorgehen Prototyp
Quelle: Eigene Darstellung, 2021

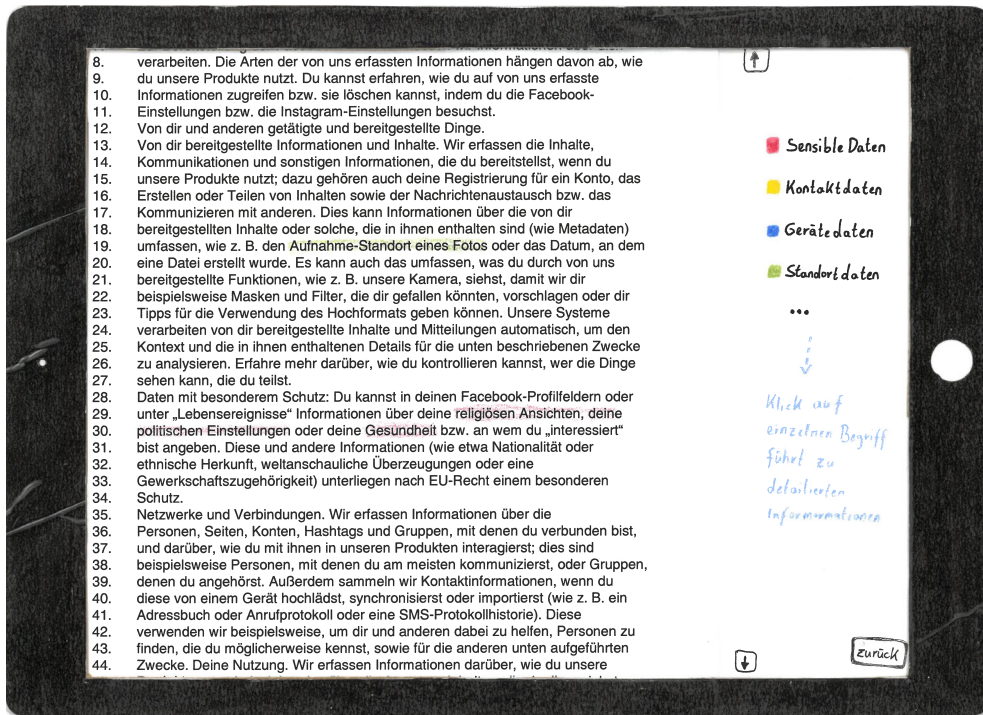


Abb. 6: Paper-Prototyp
 Quelle: Eigene Darstellung, 2021

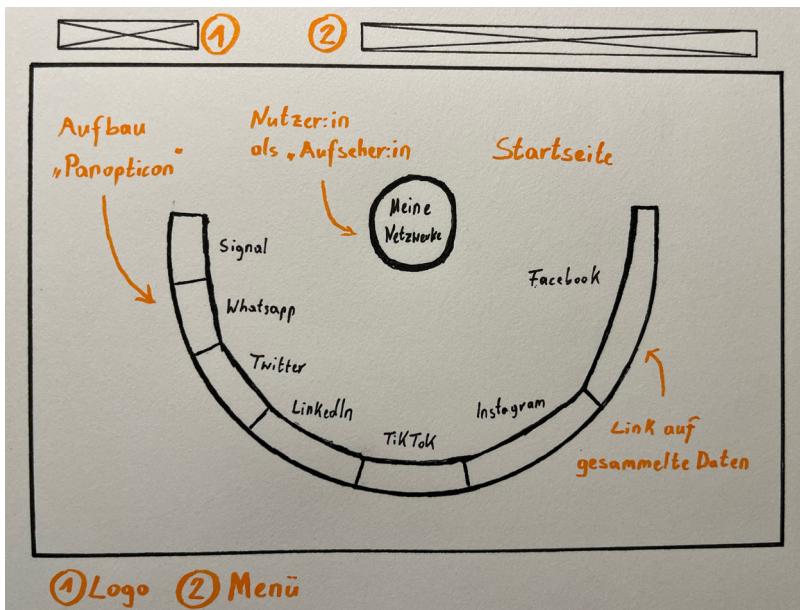


Abb. 7: Skizze Seitenaufbau Click-Dummy
 Quelle: Eigene Darstellung, 2022

2.4.3 Erstellung Click-Dummy

Unter diesem Punkt sind einige Ausschnitte des Click-Dummies abgebildet, der in Figma erstellt wurde. Das Konzept sieht die Verwendung an einem PC oder auf einem Tablet vor.

Der Prototyp besteht zum Zeitpunkt des Usability-Tests aus 15 verschiedenen Frames und deckt somit alle dafür notwendigen Funktionen ab. Zudem sind darin bereits die finalen Icons integriert.

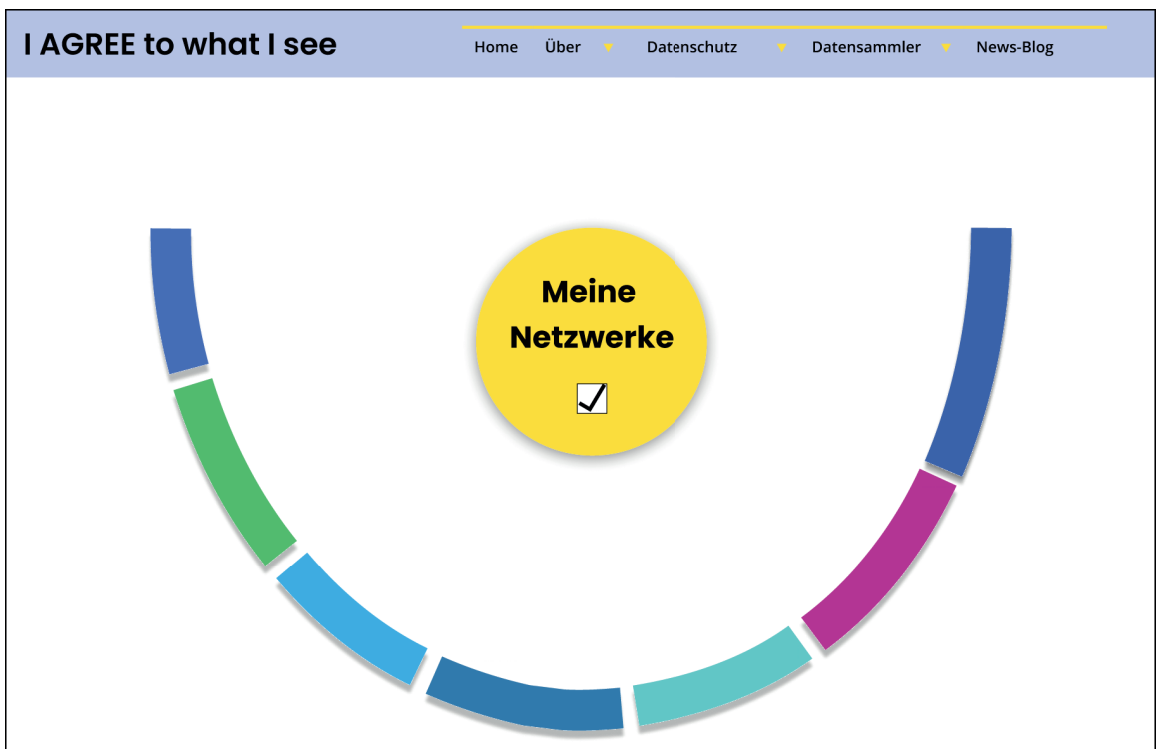


Abb. 8: Startseite Klick-Dummy *I AGREE to what I see*
Quelle: Figma, 2023, eigene Darstellung

Auf der Startseite sollen Nutzer:innen die Möglichkeit haben, ihr Social-Media-Panopticon einzurichten. Beim Prototypen sind die einzelnen sozialen Medien und Messenger-Dienste bereits festgelegt.

Mit einem Klick auf den Button *Meine Netzwerke* gelangen die Nutzer:innen auf die im folgenden abgebildete Seite.

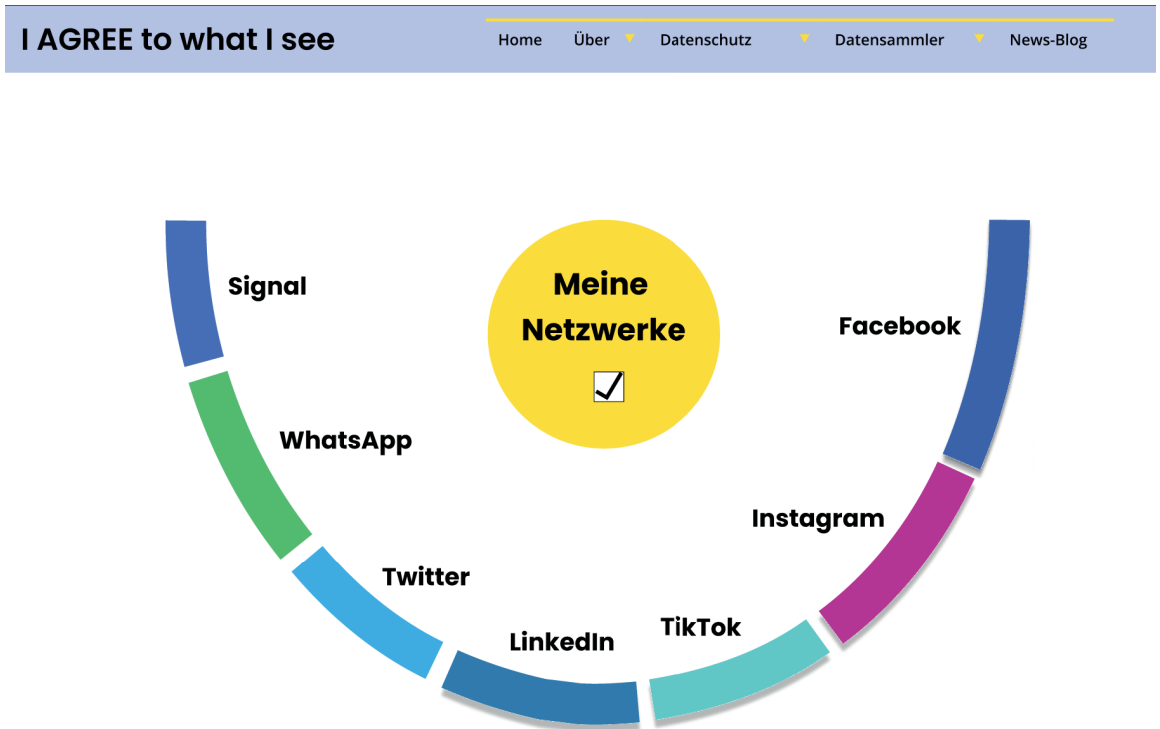


Abb. 9: Startseite Detail Klick-Dummy *I AGREE to what I see*
Quelle: Figma, 2023, eigene Darstellung

Die Farbe der jeweiligen Plattform entspricht dem des Original-Logos. Mit einem Klick auf die einzelnen Elemente gelangen die Nutzer:innen auf eine Detailseite, auf der die Datenkategorien als Icons abgebildet sind, die von dem sozialen Medium oder Messenger-Dienst gesammelt werden.

Im Folgenden ist der Aufbau des Navigations-Menüs abgebildet. Die aufgezählten Punkte sind allerdings nicht als Detailseiten im Prototyp enthalten.

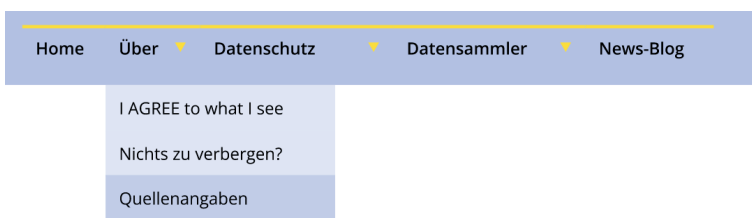


Abb. 10: Navigation Punkt *Über* Klick-Dummy *I AGREE to what I see*
Quelle: Figma, 2023, eigene Darstellung

Mit einem Klick auf eine Plattform auf der Startseite gelangen die Nutzer:innen auf eine Übersichtsseite, auf der die einzelnen Datenkategorien aufgelistet sind, die gesammelt

werden. In Abbildung 13 sind jene von Facebook und somit alle für die Arbeit erstellten Icons abgebildet. Details zu den Icons erfolgen unter Punkt 3.

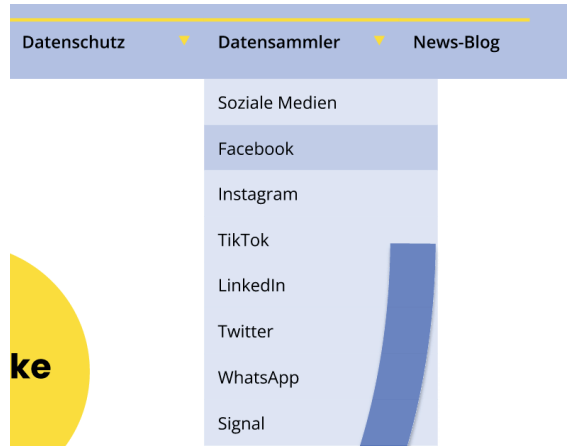
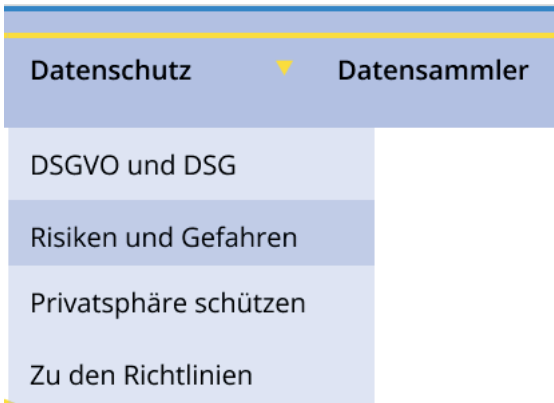


Abb. 11 (l.) und Abb. 12 (r.): Navigation *Datenschutz* und *Datensammler* Click-Dummy / *AGREE to what I see*
Quelle: Figma, 2023, eigene Darstellung

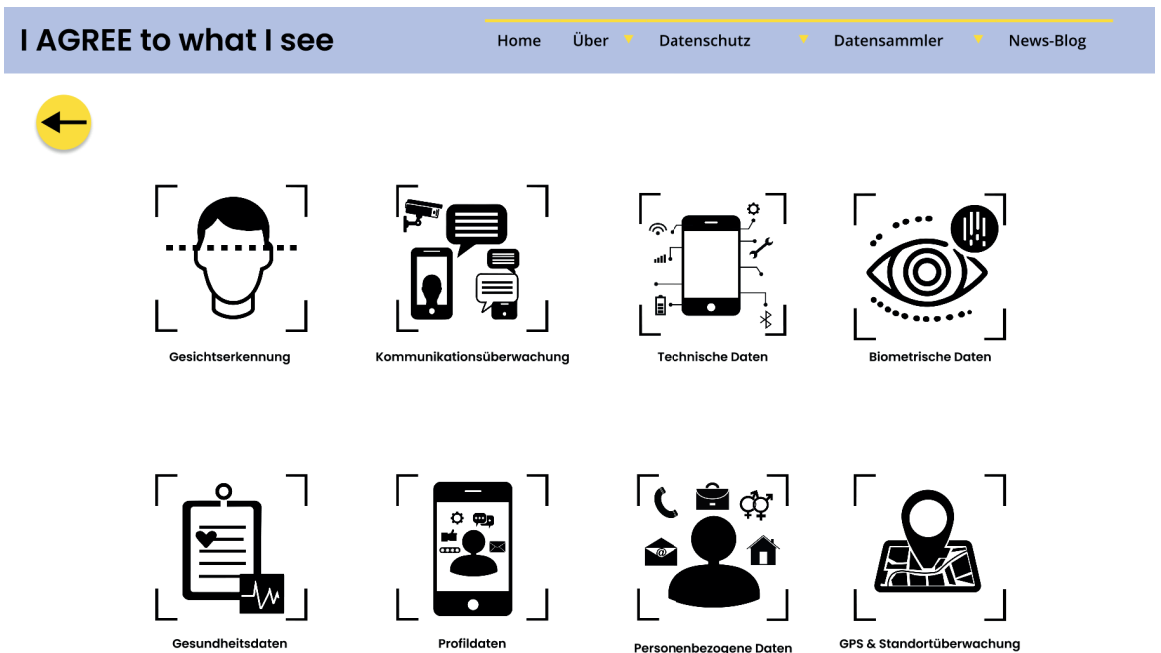




Abb. 13: Detailseite Plattform *Was wird gesammelt?* Klick-Dummy / *AGREE to what I see*
Quelle: Figma, 2023, eigene Darstellung

In Abbildung 14 ist ein Beispiel der Kategorie-Detailseiten dargestellt, auf die Nutzer:innen durch Anklicken des entsprechenden Icons gelangen. Dort finden sich genaue und möglichst einfache Beschreibungen sowie Risiken, die mit der Verarbeitung der Daten verbunden sind.

Unter Punkt 3.0 erfolgt nun die Beschreibung des methodischen Vorgehens und der Analysen, die für die Konzeption der Icons und das Forschungsvorhaben im Allgemeinen notwendig sind.

I AGREE to what I see Home Über Datenschutz Datensammler News-Blog

 **Gesichtserkennung**



Quellen

Gesichtserkennung auf sozialen Medien ist eine Funktion, bei der die Plattformen mithilfe von Algorithmen und künstlicher Intelligenz automatisch Gesichter auf Fotos oder Videos erkennen und identifizieren können. Diese Technologie analysiert die einzigartigen Merkmale des Gesichts einer Person, wie die Position der Augen, Nase und Mund, um eine eindeutige biometrische Vorlage zu erstellen.

Die Gesichtserkennung wird in sozialen Medien für verschiedene Zwecke eingesetzt:

1. **Markierung von Fotos:** Soziale Medien wie Facebook und Instagram verwenden Gesichtserkennung, um Nutzer:innen beim Hochladen von Fotos zu unterstützen, indem sie mögliche Übereinstimmungen mit den Gesichtern von Freunden oder Kontakten erkennen und vorschlagen, diese zu markieren.
2. **Sicherheit und Authentifizierung:** Einige Plattformen nutzen Gesichtserkennung als zusätzliche Sicherheitsmaßnahme zur Authentifizierung von Nutzer:innen, um sicherzustellen, dass nur autorisierte Personen Zugriff auf ihre Konten haben.
3. **Filter und Augmented Reality (AR):** Gesichtserkennung ermöglicht es auch, Filter und AR-Effekte auf Fotos oder Videos anzuwenden, um Spaß und kreative Interaktionen zu fördern.
4. **Werbung und Personalisierung:** Gesichtserkennung kann auch für personalisierte Werbung und Inhalte verwendet werden, indem sie Informationen über das Alter, das Geschlecht oder die Stimmung einer Person aus dem Gesicht ablesen.

Die Nutzung von Gesichtserkennung auf sozialen Medien wirft jedoch auch Datenschutz- und Privatsphärebedenken auf. Die Verarbeitung und Speicherung von Gesichtsdaten kann als besonders sensibel angesehen werden, da Gesichter ein eindeutiges Merkmal einer Person sind. Plattformen müssen daher transparent über ihre Gesichtserkennungspraktiken informieren und die Zustimmung der Nutzer:innen einholen, bevor sie diese Technologie verwenden.

Einige Länder haben spezifische Gesetze und Vorschriften in Bezug auf die Gesichtserkennung, um den Schutz der Privatsphäre zu gewährleisten. Benutzer:innen sollten sich der Gesichtserkennungsfunktionen bewusst sein, die auf sozialen Medienplattformen eingesetzt werden, und ihre Datenschutzeinstellungen entsprechend anpassen, wenn sie ihre Privatsphäre schützen möchten.

Obwohl die meisten sozialen Medien und Dienste die Gesichtserkennung nicht mehr explizit in ihren Datenschutzrichtlinien erwähnen, liegt es nahe, dass diese weiterhin verarbeitet werden. Gesichtserkennung zählt zu den biometrischen Daten. Diese sind nach der EU-Datenschutzgrundverordnung (Artikel 9) besonders schützenswert.

Im Gegensatz zu gestohlenen Passwörtern, die einfach geändert werden können, ist das bei biometrischen Daten nicht möglich. Gelangen sie in die falschen Hände, kann das für betroffene Personen schwerwiegende Folgen haben. Auch der staatliche Einsatz von Gesichtserkennungssoftware ist umstritten.

Abb. 14: Detailseite *Gesichtserkennung* Klick-Dummy *I AGREE to what I see*
Quelle: Figma, 2023, eigene Darstellung

„Privacy means people know what they’re signing up for, in plain language, and repeatedly. I believe people are smart. Some people want to share more than other people do. Ask them.”

Steve Jobs, CEO Apple Inc. (1955-2011)

Methodisches Vorgehen und Analyse

Befragung zur Nutzung sozialer Medien

Textanalyse nach Datenkategorien DSGVO

Cluster-Analyse

Icon-Erstellung und Testing

Testing Click-Dummy

3. Methodisches Vorgehen und Analyse

Dieses Kapitel widmet sich dem methodischen Vorgehen der Arbeit. Der erste Teil zielt darauf ab, die Nutzungsweise der Testpersonen von sozialen Medien und Messenger-Diensten sowie deren Grundkenntnisse zum Thema Datenschutz zu erörtern. Darauf aufbauend – und ergänzend durch eine Textanalyse der ausgewählten Datenschutzrichtlinien – werden 50 Begriffe definiert, die durch ein Cardsorting und der Benennung eigener Kategorien durch die Proband:innen in die Erstellung eines Dendrogramms einfließen.

Die daraus resultierenden Ergebnisse werden dann für die Gestaltung und dem Testing der Icons unter Punkt 3.4 herangezogen. Diese dienen einerseits der Beantwortung der 2. Unterforschungsfrage, welche Darstellungsformen für die Übertragung in ein informationsgrafisches System als sinnvoll erachtet werden, um den Inhalt verständlich darstellen zu können. Andererseits sind die Icons ein wesentlicher Bestandteil des Prototypens.

3.1 Befragung zur Nutzung sozialer Medien

Die mündliche Befragung in Form eines strukturierten Interviews bezweckt das Verhalten der Proband:innen bezüglich der Nutzung von sozialen Medien und Messenger-Diensten einzuschätzen sowie vorhandenes Wissen zu den Datenschutzrichtlinien abzufragen. Verhaltensfragen zielen darauf ab, herauszufinden, „was Befragte in der Vergangenheit getan haben, in der Gegenwart tun bzw. für die Zukunft zu tun beabsichtigen [...]“ (Schnell, Hill & Esser, 2008, S. 328).

Im konkreten Fall beziehen sich die Fragen auf das vergangene und gegenwärtige Verhalten.

3.1.1 Methodenwahl

Zur Durchführung des strukturierten Interviews wird ein Fragebogen mit insgesamt zehn Fragen in offener und geschlossener Form erstellt. Das Ziel ist herauszufinden, wie die Proband:innen ihr Verhalten im Umgang mit sozialen Medien und Messenger-Diensten einschätzen und welche Kenntnisse zum Thema Datenschutz bestehen. Die offenen Fragen werden in den eigenen Worten der Personen beantwortet, ohne Antwortmöglichkeiten vorzuschlagen. Bei den geschlossenen Fragen stehen zwei Möglichkeiten – *JA* und *NEIN* – zur Auswahl (Schnell, Hill & Esser, 2008, S. 330).

Die demografischen Angaben zum Geschlecht und Alter dienen lediglich der Zuordenbarkeit und lassen keine Rückschlüsse auf die befragte Person zu.

Fragebogen Nutzung sozialer Medien

Einführung/Erklärung: In dieser Befragung geht es um dein Nutzungsverhalten von sozialen Medien und Messenger-Diensten sowie um deinen Wissensstand zum Thema Datenschutz in diesem Bezug. Antworte bitte spontan auf die Fragen - es gibt kein Richtig oder Falsch.

Hinweis: Die von dir angegebenen Daten und Antworten lassen keine Rückschlüsse auf deine Person zu. Die Verarbeitung erfolgt ausschließlich zum Zweck dieses Forschungsprojekts.

Personen-Kennung:

Alter:

Geschlecht: weiblich
 männlich

1. Nutzt du soziale Medien und/oder Messenger-Dienste?

privat: JA NEIN
beruflich: JA NEIN

2. Welche sozialen Medien und Messenger-Dienste nutzt du?

privat:

beruflich:

3. Welche Daten musstest du bei der Anmeldung bei den jeweiligen Plattformen / Diensten angeben?

4. Hast du dir die Datenschutzrichtlinie der jeweiligen Plattform / des jeweiligen Dienstes durchgelesen?

JA

NEIN

5. Wenn JA / NEIN, warum?

6. Was glaubst du, welche Daten die jeweiligen Unternehmen von dir sammeln?

7. Siehst du darin irgendwelche Gefahren oder Risiken für dich?

8. Gibt es Informationen, die du lieber nicht mit diesen Unternehmen teilen möchtest?

9. Wäre ein Leben ohne soziale Medien und Messenger-Dienste für dich vorstellbar?

JA

NEIN

10. Wenn JA / NEIN, warum?

Vielen Dank für das Gespräch!



3.1.2 Ablauf

Die Befragung der 10 Teilnehmer:innen, zum Zeitpunkt im Alter zwischen 17 und 73 Jahren, erfolgt persönlich. Die Antworten werden während des Gesprächs von der Verfasserin mitdokumentiert. Zu Beginn werden die Teilnehmer:innen über den Zweck und das Ziel des Interviews informiert.

Die Auswertung sowie eine Zusammenfassung der Antworten sind im nächsten Punkt abgebildet. Die ausgefüllten Fragebögen aller Teilnehmer:innen finden sich im Anhang.

3.1.3 Auswertung und Ergebnisse

Teilnehmer:innen:

6 weiblich

4 männlich

Frage zur Nutzung sozialer Medien und Messenger-Dienste.

privat: 

beruflich: 

100 Prozent der Befragten geben an, zumindest ein soziales Medium oder einen Messenger-Dienst privat zu nutzen. Beruflich liegt die Nutzung bei 50 Prozent.

Frage, ob zumindest eine Datenschutzrichtlinie gelesen wurde.

JA: 

NEIN: 

Zwei Personen (20 Prozent) gaben an, zumindest eine Richtlinie angelesen bzw. überflogen zu haben.

Frage, ob ein Leben ohne soziale Medien und Messenger-Dienste vorstellbar wäre.

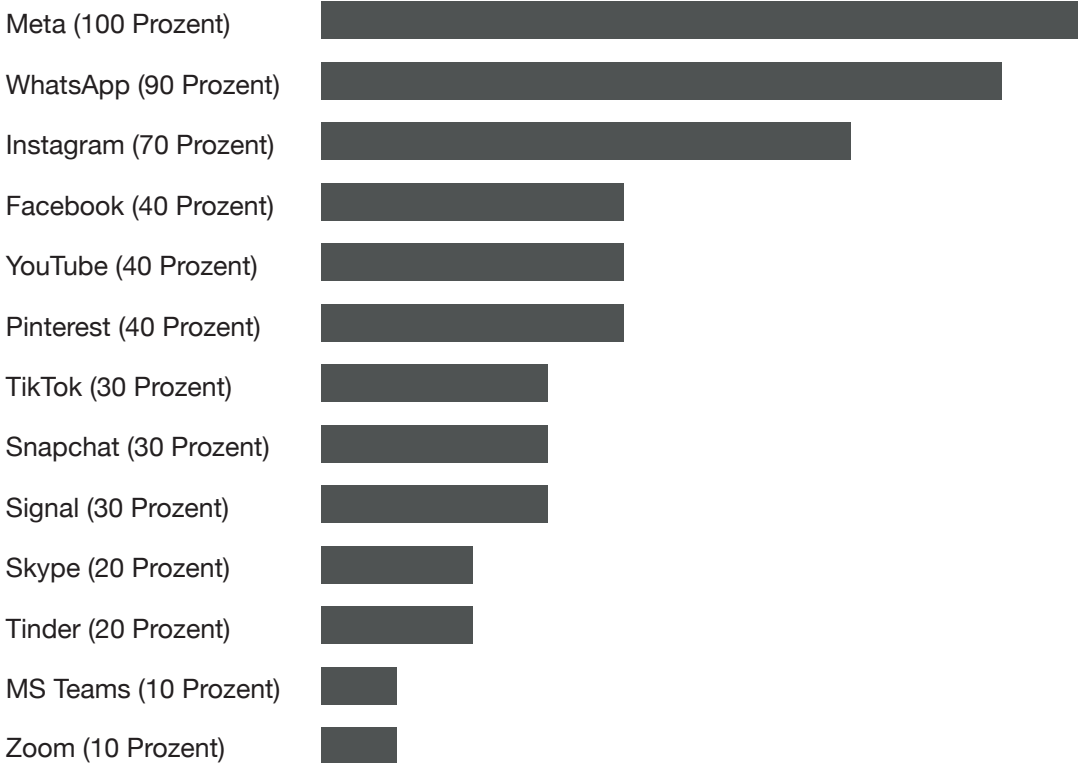
JA: 

NEIN: 

Rund 30 Prozent der Befragten geben an, dass sie unter Umständen auf soziale Medien und Messenger-Dienste verzichten könnten. Für 70 Prozent ist das nicht vorstellbar.

Von den Teilnehmer:innen genutzte soziale Medien und Messenger Dienste:

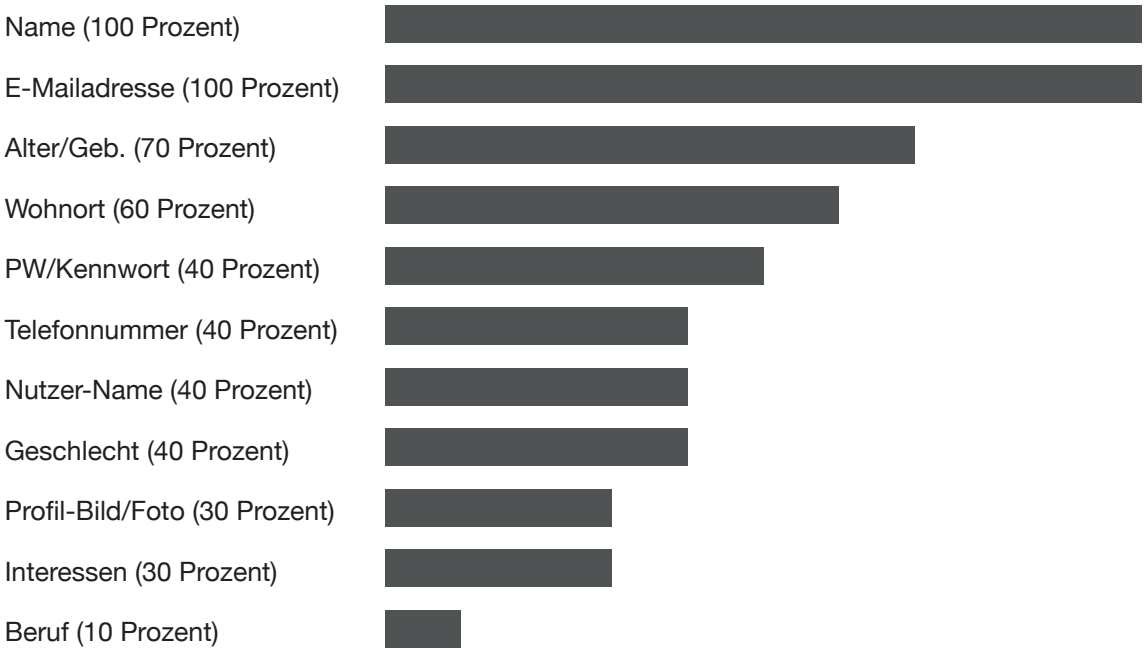
Privat-Nutzung:



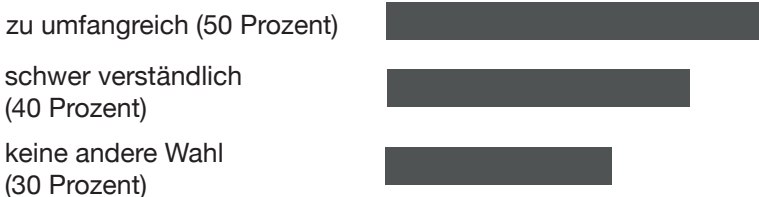
Berufliche Nutzung:



Frage, welche Daten bei der Anmeldung eines Dienstes angegeben werden müssen.



Frage, warum Datenschutzrichtlinien gelesen wurden oder warum nicht. Die Aufzählungen sind nur ein Ausschnitt der gegebenen Antworten aus den Fragebögen und somit nicht vollständig. (Quelle siehe Anhang)



zu mühsam (50 Prozent)

noch keine Gedanken darüber gemacht (20 Prozent)

Antworten auf die Frage, welche Daten die Betreiber der sozialen Medien und Messenger-Dienste von den Befragten sammeln (nur explizite Nennungen).

Persönliche Daten (80 Prozent)

Kommentare/Nachrichten (70 Prozent)

Alles, was sie kriegen können (50 Prozent)

Bilder inkl. Profilbild (30 Prozent)

Bewegungsdaten (20 Prozent)

Suchverläufe (10 Prozent)

Onlinezeit (10 Prozent)

Kontakte (10 Prozent)

Kaufverhalten (10 Prozent)

Antworten auf die Frage, was nicht auf sozialen Medien und Messenger-Diensten geteilt werden möchte (einige Antworten wurden in einem Überbegriff zusammengefasst).

Gehalt (40 Prozent)

Bank-/Finanz- und Kontodaten (30 Prozent)

Details aus Intim- bzw. Privatleben (30 Prozent)

Biometrische Daten (20 Prozent)

Politische Einstellung (10 Prozent)

Sexuelle Orientierung (10 Prozent)

3.2 Textanalyse nach Datenkategorien DSGVO

Die Analyse der Texte soll einen groben Überblick deren Inhalte ermöglichen. Wie bereits erwähnt, unterscheidet die DSGVO unter anderem zwischen der Verarbeitung der allgemeinen personenbezogenen Daten und der Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 (EU 2016/679). Für eine genaue Analyse der Datenrichtlinien der sozialen Medien und Messenger-Dienste sind diese beiden Überkategorien allerdings zu wenig aussagekräftig. Aus diesem Grund erfolgt eine weitere Unterteilung in insgesamt fünf Kategorien:

- Personenbezogene Daten nach Art. 9 DSGVO
- Nutzer:innen-Daten wie Name, Profilname, Adresse, Geburtsdatum und Profilbild
- Technische Daten wie IP-Adresse, Geräteinformationen, verwendetes Betriebssystem, Metadaten u. ä.
- Geo-Daten (z. B. Standort, Einsatz von GPS)
- Profiling Daten wie verbundene Konten, verwendete Hashtags, Gruppen, Interaktionen usw., die vor allem der Generierung von personenzentrierter Werbung dienen und sich häufig wieder auf Daten nach Artikel 9 der DSGVO zurückführen lassen.

3.2.1 Methodenwahl

Die Textanalyse erfolgt in zwei Schritten. Zunächst wird eine Prüfung der Datenschutzrichtlinien über den Lesbarkeitsindex (LIX) durchgeführt, um die Komplexität dieser Texte besser abbilden zu können. Dieser wurde 1968 von Carl-Hugo Björnsson entwickelt und bestimmt anhand verschiedener Textmerkmale (z. B. Satz- und Wort-Länge) deren Schwierigkeit. Je höher der LIX-Wert, umso komplexer

und schwieriger der Text. Im Folgenden ein Vergleich mit Textgattungen, die den ungefähren Einschätzungen der Textschwierigkeit entsprechen:

unter 40: Kinder- und Jugendliteratur
40 bis 50: Belletristik
50 bis 60: Sachliteratur
über 60: Fachliteratur

(Lenhard, A., & Lenhard, W. (2017).

Mittels qualitativer Analysemethoden werden im zweiten Schritt Inhalte der Datenschutzrichtlinien Anhand der fünf genannten Kategorien auf relevante Datensätze untersucht. Daten, die den Nutzer:innen unter Umständen verborgen bleiben, werden so sichtbar gemacht und wahrgenommen. Zudem werden bei dieser Analyse 50 Begriffe aus den Datenschutzrichtlinien für das Card-sorting und die Cluster-Analyse unter Punkt 3.3 bestimmt.

3.2.2 Ablauf

Für die Durchführung der Textanalyse werden die Datenschutzrichtlinien der ausgewählten Plattformen zunächst in ein MS Word-File eingefügt.

Zur Überprüfung des Lesbarkeitsindex werden die Inhalte in das Eingabefeld der Webseite Psychometrica eingefügt und ausgewertet (Lenhard, A., & Lenhard, W. (2017). Anschließend erfolgt die Übertragung der Ergebnisse in eine Tabelle (siehe Punkt 3.2.3).

Für die qualitative Analyse der Texte werden diese durchgearbeitet und auf die definierten Datenschutz-Kategorien geprüft. Entsprechende Passagen der Richtlinien werden markiert. Die gesamten Auswertungen der Richtlinien finden sich im Anhang.

3.2.3 Auswertung und Ergebnisse

Prüfung Lesbarkeitsindex (LIX) der Datenschutzrichtlinien:

Plattform	Anzahl Wörter	Anzahl Sätze	LIX-Wert	Komplexität
Meta (Facebook und Instagram)	22.245	1.206	58.51	hoch
TikTok	5.288	322	55.93	hoch
LinkedIn	6.528	354	58.61	hoch
Twitter	4.372	231	54.95	mittel
WhatsApp	10.707	601	60.37	hoch
Signal	524	46	46.7	mittel

Tabelle 2: LIX-Werte Datenschutzrichtlinien

Quelle: Auswertung Psychometrica Lesbarkeits-Index, 2022, eigene Darstellung

Ein Wert von über 50 oder 60 entspricht dem Lesbarkeitsindex nach Sach- und Fachliteratur. Zurückzuführen ist dies unter anderem auf die Satzlänge, Anzahl der Wörter, Abkürzungen, aber auch Fachbegriffe (Lenhard, A., & Lenhard, W. (2017).

Qualitative Textanalyse Datenschutzrichtlinien:

- **Inhaltliche Merkmale und Eigenschaften.** Wir erkennen und erheben Merkmale und Eigenschaften der Video- und Audioaufnahmen, die Teil deiner **Nutzerinhalte** sind, z. B. durch die Identifizierung von Objekten und Landschaften, das Vorhandensein oder die Position eines Gesichts oder anderer Körperteile innerhalb eines Bildes und den Text der in deinen Nutzerinhalten gesprochenen Wörter. Wir tun dies zum Beispiel für die Moderation von Inhalten und zur Bereitstellung von Spezialeffekten (wie Videofilter und Avatare) und Untertiteln.

Abb. 16: Auszug Datenschutzrichtlinien TikTok

Quelle: TikTok Datenschutzrichtlinie, 2022

Bei der Textanalyse wird festgestellt, dass Plattformen wie Facebook, Instagram und TikTok sowie der Messenger Dienst WhatsApp eine große Anzahl verschiedenster Daten von Nutzer:innen abfragen, sammeln und verarbeiten. Die entsprechenden Textpassagen werden dabei mehrmals wiederholt. Die Abbildung unten zeigt einen Auszug der TikTok-Datenschutzrichtlinie zur automatischen

Erfassung von Daten. Die darin beschriebene Erfassung der Position eines Gesichts sowie anderer Körperteile in Bildern deutet ein Stück weit auf den Einsatz von Gesichtserkennungstechnologien hin. Dabei handelt es sich um die Erfassung biometrischer Daten, die unter die besonderen Kategorien personenbezogener Daten gemäß Artikel 9 der DSGVO fallen und somit als besonders schützenswert gelten.

3.3 Cluster-Analyse

Mit der Textanalyse können bereits wichtige Informationen in den verschiedenen Datenschutzrichtlinien extrahiert werden. Insgesamt werden 50 verschiedene Begriffe ausgewählt, anhand derer ein Cardsorting durchgeführt wird. Die Ergebnisse fließen in die Cluster-Analyse mit ein. Diese folgt dem Zweck, durch die individuelle Strukturierung der Nutzer:innen möglicherweise neue Überkategorien benennen zu können, die in weiterer Folge auch in die Entwicklung des Zeichensystems miteinfließen können. Hierbei steht vor allem John Maedas Ansatz von SORT, LABEL, INTEGRATE und PRIORITIZE im Vordergrund, um die Informationen möglichst präzise und strukturiert darstellen und weiterverarbeiten zu können (Maeda, 2006, S. 13f).

3.3.1 Methodenwahl

Für die Kategorisierung der 50 Begriffe wird ein offenes Cardsorting durchgeführt. Bei diesem generativen Ansatz sortieren die Testpersonen die Wörter in für sie zusammengehörige Gruppen und benennen diese. Das Cardsorting eignet sich besonders für die Generierung von quantitativen und qualitativen Aussagen und ist ein wesentlicher Bestandteil nutzer:innenzentrierter Entwicklungen (Sinnig, 2020).

Folgende 50 Begriffe in der Tabelle werden kategorisiert:

1	Mobilfunkanbieter	18	Persönliche Nachrichten	35	Gesundheitsdaten
2	Geräte-ID	19	Kaufverhalten	36	Sexuelle Orientierung
3	Name	20	Nutzername	37	Biometrische Daten
4	E-Mailadresse	21	Kontakte	38	Genutzte Geräte
5	Wohnort	22	Freunde	39	Telefonmarke
6	Alter	23	Beiträge/Postings	40	TelefonEinstellungen
7	Geburtsdatum	24	Verweildauer	41	Verwendetes Betriebssystem
8	Gesichtserkennung	25	#Hashtags	42	IP-Adresse
9	Besuchte Webseiten	26	Likes	43	Nationalität
10	Persönliches Adressbuch	27	Reaktionen (Emojis)	44	Interessen
11	Geo-Tag	28	Profil-Foto	45	Geschlecht
12	Zahlungsinformation	29	Hochgeladene Files/Videos	46	Beruf
13	Gesendete Nachrichten	30	Follower	47	Politische Ansichten
14	Chatnachrichten	31	Interaktionen	48	Religiöse Ansichten
15	Anrufprotokoll	32	Markierungen (Tags)	49	Gewerkschaftszugehörigkeit
16	Gespeicherte Cookies	33	Gruppen (öffentlich/privat)	50	Ethnische Herkunft
17	GPS-Standort	34	Kommentare		

Tabelle 3: Begriffe Card-Sorting

Quelle: Datenschutzrichtlinien Meta - Facebook, Instagram (2023), TikTok (2022), LinkedIn (2020), Twitter (2022), Meta-WhatsApp (2022), Signal, EU Verordnung 2016/679

3.3.2 Ablauf

Das Cardsorting wird mit 20 Personen (13 weiblich, 7 männlich) im Alter zwischen 20 und 73 Jahren durchgeführt. Alle Teilnehmer:innen nutzen zumindest eine der in dieser Arbeit analysierten Plattformen.

Die Sortierung erfolgt in Excel. Alle Teilnehmer:innen füllen die Tabelle nach einer kurzen Erklärung selbstständig aus. Die einzelnen Dateien werden anschließend in eine gemeinsame überführt.

In der Tabelle 4 ist ein Auszug aus den durchgeführten Cardsortings dargestellt:

Die Auswertung des Cardsortings erfolgt in RStudio. Dabei handelt es sich um eine integrierte Entwicklungsumgebung und grafische Benutzeroberfläche, in der unter anderem die Statistik-Programmiersprache R zum Einsatz kommt (Posit – The Open-Source Data, 2023). Zur Analyse wird die Excel-Datei mit den Ergebnissen des Cardsortings in RStudio importiert.

Der Code inklusive Beschreibung findet sich im Anhang. Aus den Ergebnissen des Cardsortings wird mithilfe einer hierarchischen Cluster-Analyse in RStudio ein Dendrogramm erstellt, das im nächsten Punkt genauer beschrieben wird.

B	C	D	E	F	G	H	I
Nr.	Bezeichnung	ID1	ID2	ID3	ID4	ID5	ID6
1	Mobilfunkanbieter	Geräte-Daten	Technische Daten	Geräte-Daten	Technische Daten;	Geräte-Daten	Mobil-Daten
2	Geräte-ID	Geräte-Daten	Technische Daten	Geräte-Daten	Technische Daten	Geräte-Daten	Mobil-Daten
3	Name	Persönliche Daten	Persönliche Daten	Kontaktdaten	Anschrift-Daten	Allgemeine Daten	Kontakt-Daten
4	E-Mailadresse	Persönliche Daten	Persönliche Daten	Kontaktdaten	Anschrift-Daten	Allgemeine Daten	Kontakt-Daten
5	Wohnort	Persönliche Daten	Persönliche Daten	Kontaktdaten	Anschrift-Daten	Allgemeine Daten	Kontakt-Daten
6	Alter	Persönliche Daten	Persönliche Daten	Kontaktdaten	Persönliche Daten	Allgemeine Daten	Kontakt-Daten
7	Geburtsdatum	Persönliche Daten	Persönliche Daten	Kontaktdaten	Persönliche Daten	Allgemeine Daten	Kontakt-Daten
8	Gesichtserkennung	Überwachungsdaten	Private Daten	Überwachungsdaten	Höchstpersönliche Daten	Private Daten	Persönliche Daten
9	Besuchte Webseiten	Überwachungsdaten	Technische Daten	Überwachungsdaten	Technische Daten	Private Daten	Bewegungs-Daten
10	Persönliches Adressbuch	Private Daten	Persönliche Daten	Überwachungsdaten	Persönliche Daten	Private Daten	Persönliche Daten
11	Geo-Tag	User-Aktion	Ortungs-Daten	Überwachungsdaten	Standortdaten	Geräte-Daten	Bewegungs-Daten
12	Zahlungsinformation	Private Daten	Persönliche Daten	Überwachungsdaten	Persönliche Daten	Private Daten	Persönliche Daten
13	Gesendete Nachrichten	User-Interaktion	Private Daten	Überwachungsdaten	Persönliche Daten	Private Daten	Persönliche Daten
14	Chatnachrichten	User-Interaktion	Private Daten	Überwachungsdaten	Persönliche Daten	Private Daten	Mobil-Daten
15	Anrufprotokoll	Überwachungsdaten	Private Daten	Überwachungsdaten	Persönliche Daten	Geräte-Daten	Mobil-Daten
16	Gespeicherte Cookies	Überwachungsdaten	Technische Daten	Überwachungsdaten	Technische Daten	Geräte-Daten	Geräte-Daten
17	GPS-Standort	Überwachungsdaten	Ortungs-Daten	Überwachungsdaten	Standortdaten	Geräte-Daten	Bewegungs-Daten
18	Persönliche Nachrichten	User-Interaktion	Private Daten	Überwachungsdaten	Persönliche Daten	Private Daten	Aktions-Daten
19	Kaufverhalten	User-Gruppierung	Private Daten	Überwachungsdaten	Persönliche Daten	Private Daten	Persönliche Daten
20	Nutzername	User-Aktion	Profil-Daten	Profil-Daten	Profil-Daten	Plattform-Daten	Profil-Daten

Tabelle 4: Auszug Cardsorting

Quelle: Excel, 2022, eigene Darstellung

3.3.3 Auswertung und Ergebnisse

Die hierarchische Cluster-Analyse ergibt ein Dendrogramm (siehe Abbildung 17), mit insgesamt vier Clustern verschiedener Größe.

Die Nummern entsprechen dem jeweiligen Begriff in der Excel-Tabelle. In Tabelle 5 sind die vier Cluster mit den ihnen zugeordneten Begriffen von links nach rechts abgebildet.

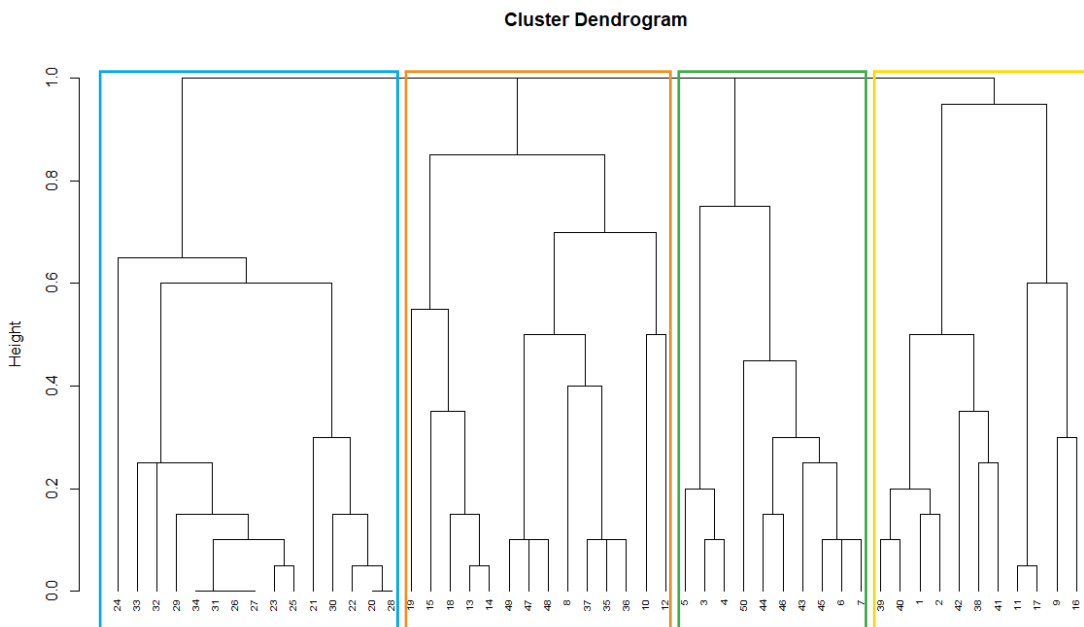


Abb. 17: Cluster Dendrogramm
Quelle: RStudio-Auswertung, 2022, eigene Darstellung

Cluster 1 (blau)	15 Begriffe	Verweildauer, Gruppen (öffentlich/privat), Markierungen (Tags), Hochgeladene Files/Videos, Kommentare, Interaktionen, Likes, Reaktionen (Emojis), Beiträge/Postings, #Hashtags, Kontakte, Follower, Freunde, Nutzernamen, Profilfoto
Cluster 2 (orange)	14 Begriffe	Kaufverhalten, Anrufprotokoll, Persönliche Nachrichten, Gesendete Nachrichten, Chatnachrichten, Gewerkschaftszugehörigkeit, Politische Ansichten, Religiöse Ansichten, Gesichtserkennung, Biometrische Daten, Gesundheitsdaten, Sexuelle Orientierung, Persönliches Adressbuch, Zahlungsinformation
Cluster 3 (grün)	10 Begriffe	Wohnort, Name, E-Mailadresse, Ethnische Herkunft, Interessen, Beruf, Nationalität, Geschlecht, Alter, Geburtsdatum
Cluster 4 (gelb)	11 Begriffe	Telefonmarke, Telefoneinstellungen, Mobilfunkanbieter, Geräte-ID, IP-Adresse, Genutzte Geräte, Verwendetes Betriebssystem, Geo-Tag, GPS-Standort, Besuchte Webseiten, Gespeicherte Cookies

Tabelle 5: Cluster-Auswertung
Quelle: Eigene Darstellung, 2022

Cluster 1 (blau) umfasst größtenteils Begriffe, die mit einer Aktivität bzw. Interaktion der Nutzer:innen auf sozialen Medien verbunden sind. Er könnte somit als Profildaten-Cluster bezeichnet werden. Die Aufteilung erfolgt in zwei größere Untergruppen ausgenommen der *Verweildauer*, die einen einzelnen Strang bildet.

In Cluster 2 (orange) finden sich, bis auf den Begriff der *Ethnischen Herkunft*, alle sensiblen Daten aus Artikel 9 der DSGVO (EU Verordnung 2016/679). Darin finden sich auch alle Daten, die mit privater Kommunikation und Finanzen (*Kaufverhalten, Zahlungsinformation*) in Verbindung gebracht werden können. Die *biometrischen Daten, Gesundheitsdaten* und die *sexuelle Orientierung* sowie *Gewerkschaftszugehörigkeit, politische* und *religiöse Ansichten* bilden jeweils eine gemeinsame Untergruppe. Dazwischen liegt ein einzelner Strang mit der *Gesichtserkennung*.

Als Überbegriff kann für den 2. Cluster Personenbezogene Daten oder Private Daten gewählt werden.

Der dritte Cluster (grün) enthält hauptsächlich demografische Daten. Auch hier besteht häufig ein Personenbezug, im Vergleich zu den Daten in Cluster 2 allerdings weniger auf persönlicher bzw. privater Ebene. Auffallend ist, dass der Begriff der *Ethnischen Herkunft* dieser Gruppe zugeordnet wird. Er ist somit der einzige Datenwert der besonders schützenswerten Daten nach Art. 9 EU-Datenschutzgrundverordnung, der sich in einem gesonderten Cluster befindet (EU Verordnung 2016/679).

Im 4. großen Cluster sind vor allem technische bzw. technikbezogene Daten gruppiert. Bei der Betrachtung der Untergruppen fällt auf, dass beispielsweise die Begriffe *Telefonmarke, Telefoneinstellungen, Mobilfunkanbieter und Geräte-ID* zusammengefasst werden. Eine ähnliche Gruppierung findet sich auch bei den Begriffen *Geo-Tag* und *GPS-Standort* sowie *Besuchte Webseiten* und *Gespeicherte Cookies*. Die *genutzten Geräte* und das *verwendete Betriebssystem* werden ebenfalls in Verbindung gebracht, einzig die *IP-Adresse* bildet einen Einzelstrang.

Anschließend an die Cluster-Auswertung erfolgt die Zusammenfassung der Kategorie-Namen, die von den Teilnehmer:innen des Cardsortings definiert werden. Das Ziel ist, die insgesamt 42 Bezeichnungen auf maximal 10 Kategorien zu reduzieren, für die im nächsten Punkt entsprechende Icons entworfen und getestet werden.

Die zunächst recht hohe Zahl an Bezeichnungen liegt daran, dass viele Kategorienamen recht ähnlich gewählt wurden, z. B. Technische Daten und Technik-Daten, Sensible Daten und empfindliche Daten, Personenbezogene Daten und Persönliche Daten und so

weiter (siehe Tabelle 6). Anhand der Auswertungen und Zusammenfassung ähnlicher Begriffe können schlussendlich acht Kategorien für die Icons definiert werden, die unter Punkt 3.4 entworfen und getestet werden. Diese lauten wie folgt:

- Gesichtserkennung
- Biometrische Daten
- Kommunikationsüberwachung
- Gesundheitsdaten
- GPS- & Standortüberwachung
- Personenbezogene Daten
- Profil-Daten
- Technische Daten

Nutzer:innen-Kategorien	Anzahl Einträge	Bezeichnung in Richtlinien
Geräte-Daten	61	Mobilfunkanbieter, Geräte-ID, Telefon-Marke, Telefon-Einstellungen, Genutzte Geräte, Verwendetes Betriebssystem, IP-Adresse, Geo-Tag, Anrufprotokoll, Gespeicherte Cookies, GPS-Standort, Verweildauer, Kontakte
Mobil-Daten	6	Mobilfunkanbieter, Geräte-ID, Chatnachrichten, Anrufprotokoll, Genutzte Geräte, Telefonmarke
Technische Daten	72	Mobilfunkanbieter, Geräte-ID, Gesichtserkennung, Gespeicherte Cookies, Genutzte Geräte, Telefonmarke, Telefon-Einstellungen, Verwendetes Betriebssystem, IP-Adresse, Verweildauer, Zahlungsinformation, Anrufprotokoll, Geo-Tag, GPS-Standort
Hersteller-Daten	4	Geräte-ID, Telefoneinstellungen, Verwendetes Betriebssystem, IP-Adresse
Personenbezogene Daten	26	Name, E-Mailadresse, Wohnort, Alter, Geburtsdatum, Persönliches Adressbuch, Nationalität, Interessen, Geschlecht, Beruf, Ethnische Herkunft, Besuchte Webseiten, Zahlungsinformation, Gespeicherte Cookies, IP-Adresse
Persönliche Daten	113	Name, E-Mailadresse, Wohnort, Alter, Geburtsdatum, Nationalität, Geschlecht, Beruf, Persönliches Adressbuch, Zahlungsinformation, Interessen, Politische Ansichten, Religiöse Ansichten, Gewerkschaftszugehörigkeit, Ethnische Herkunft, Gesendete Nachrichten, Chatnachrichten, Anrufprotokoll, Persönliche Nachrichten, Kaufverhalten, Gesichtserkennung, Gesundheitsdaten, Sexuelle Orientierung, Biometrische Daten, Kontakte, Nutzernamen, Freunde, Beiträge/Postings, Profil-Foto, Hochgeladene Files/Videos

Tabelle 6: Auszug Auswertung Nutzer:innen-Kategorien
Quelle: Eigene Darstellung, 2022

3.4.2 Umsetzung

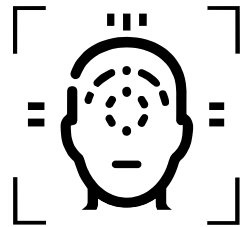
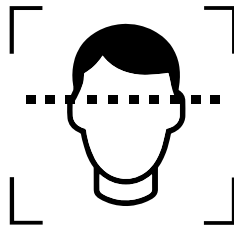
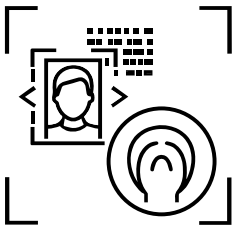
Damit die Vereinheitlichung des Zeichensystems, also der Icons, gewährleistet werden kann, werden folgende Rahmenbedingungen definiert:

Die Größe der Icons soll 30 mal 30 mm betragen. Damit sind sie auch im Klick-Dummy gut erkennbar. Sie werden ausschließlich in der Farbe schwarz auf weißem Hintergrund gehalten, da der Einsatz von Farben ablenkend wirken und einen spielerischen Eindruck

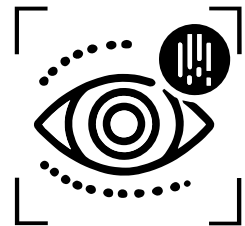
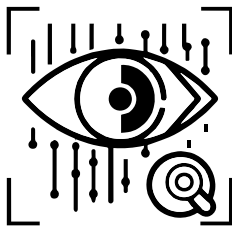
vermitteln könnte. Da mit den Icons allerdings Wissen vermittelt werden soll, wird ein möglichst neutraler Gestaltungsansatz gewählt. Für den Rahmen wird eine quadratische Kontur gewählt, allerdings wird dieser nur in den Ecken angedeutet. Im Gegensatz zur abgerundeten Form wirkt dieser Ansatz technischer und somit weniger verspielt.

Für jede der insgesamt acht Kategorien werden jeweils drei Varianten an Icons entworfen. Diese sind im Folgenden bzw. auf der nächsten Seite abgebildet.

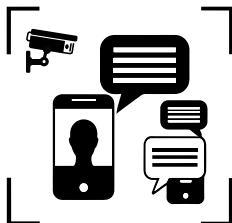
Gesichtserkennung:



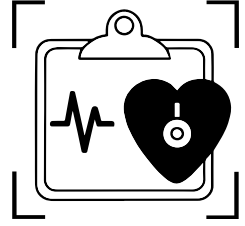
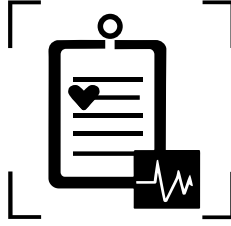
Biometrische Daten:



Kommunikationsüberwachung:



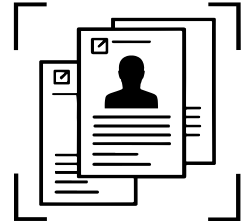
Gesundheitsdaten:



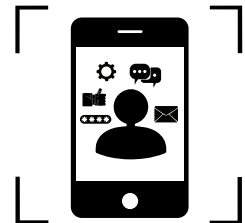
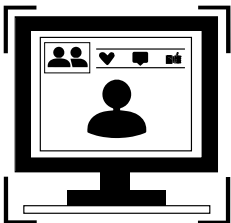
GPS- & Standortüberwachung:



Personenbezogene Daten:



Profildaten:



Technische Daten:

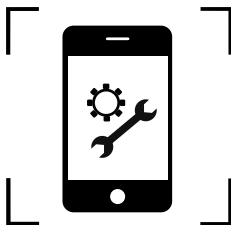
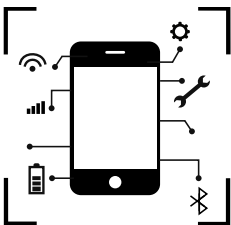


Abb. 19-42: Icon-Entwürfe für Usability Testing
Quelle: Eigene Darstellung, 2022

3.4.3 Methodenwahl

Die entworfenen Icons sollen nun einem Icon-Usability-Test unterzogen werden. Der Fokus liegt dabei auf zwei Qualitätskriterien: der Erkennbarkeit und der Ästhetik (Harley, 2016). Obwohl letztere weniger Gewichtung hat, trägt sie dennoch ihren Teil zur Vermittlung des Inhalts bei. Das Ziel ist, jeweils einen Icon aus den acht definierten Kategorien herauszufiltern, der schlussendlich auch im Prototypen zum Einsatz kommen soll.

3.4.4 Ablauf

Den zwölf Teilnehmer:innen (vier weiblich, acht männlich) im Alter zwischen 22 und 54 Jahren wird ein Fragebogen vorgelegt, in dem jeweils die drei Varianten jeder Kategorie abgebildet sind. Im ersten Schritt sollen die Erkennbarkeit mit „sehr gut erkennbar“, „gut erkennbar“, „weniger/gar nicht erkennbar“ bewertet werden. Im Gegensatz zu klassischen Erkennbarkeits-Testings wird die Kategorie-Bezeichnung genannt (Harley, 2016). Die Teilnehmer:innen sollen also abwägen, welches Icon am ehesten den genannten Begriff repräsentiert.

Bei der zweiten Frage des Testings soll die Ästhetik bewertet werden. Die Teilnehmer:innen können hierbei zwischen „sehr ansprechend“, „ansprechend“ und „wenig/nicht ansprechend“ auswählen. Die Fragebögen werden in Abwesenheit der Verfasserin händisch von den Teilnehmer:innen ausgefüllt und

anschließend ausgewertet. Die Exemplare sind dem Anhang beigefügt. Auf der folgenden Seite ist ein Auszug des für das Testing verwendeten Fragebogens abgebildet. Die restlichen Befragungen zu den Icons sind ident aufgebaut.

3.4.5 Auswertung und Ergebnisse

Für die Auswertung des Usability-Testings der Icons wird folgendes Bewertungs-Schema angewendet:

	Auswahl	Punkte
Erkennbarkeit	sehr gut erkennbar	3
	gut erkennbar	2
	wenig/gar nicht erkennbar	1
Ästhetik	sehr ansprechend	3
	ansprechend	2
	wenig/gar nicht ansprechend	1

Tabelle 7: Bewertungs-Schema Usability-Testing Icons
Quelle: Eigene Darstellung, 2022

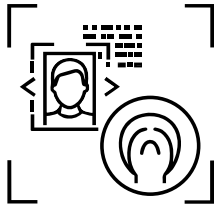
Die Auswertung der vergebenen Punkte erfolgt in einer Excel-Datei. In jeder der acht Kategorien wird somit das Icon mit dem höchsten Wert für den Einsatz im Klick-Dummy ausgewählt. Auf Seite 67 sind alle Ergebnisse des Usability-Testings dargestellt.

Icon Präferenz- und Ästhetik-Testing

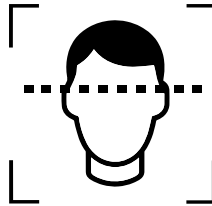
Welches der jeweils drei gezeigten Beispiele repräsentiert für dich am ehesten den genannten Begriff? Bewerte dafür jeden Icon mit „sehr gut erkennbar“, „gut erkennbar“ und „wenig/gar nicht erkennbar“. Bewerte anschließend in jedem Beispiel die Ästhetik der Icons mit „sehr ansprechend“, „ansprechend“ und „weniger/gar nicht ansprechend“.

Gesichtserkennung

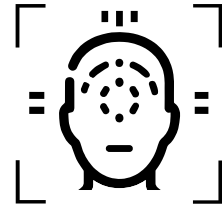
Wie gut oder schlecht erkennst du den Begriff „Gesichtserkennung“ in den gezeigten Beispielen?



- sehr gut erkennbar
 gut erkennbar
 wenig/gar nicht erkennbar



- sehr gut erkennbar
 gut erkennbar
 wenig/gar nicht erkennbar



- sehr gut erkennbar
 gut erkennbar
 wenig/gar nicht erkennbar

Wie (ästhetisch) ansprechend ist der jeweilige Icon für dich?

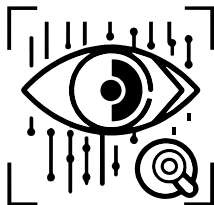
- sehr ansprechend
 ansprechend
 wenig/nicht ansprechend

- sehr ansprechend
 ansprechend
 wenig/nicht ansprechend

- sehr ansprechend
 ansprechend
 wenig/nicht ansprechend

Biometrische Daten

Wie gut oder schlecht erkennst du den Begriff „Biometrische Daten“ in den gezeigten Beispielen?



- sehr gut erkennbar
 gut erkennbar
 wenig/gar nicht erkennbar



- sehr gut erkennbar
 gut erkennbar
 wenig/gar nicht erkennbar



- sehr gut erkennbar
 gut erkennbar
 wenig/gar nicht erkennbar

Wie (ästhetisch) ansprechend ist der jeweilige Icon für dich?

- sehr ansprechend
 ansprechend
 wenig/nicht ansprechend

- sehr ansprechend
 ansprechend
 wenig/nicht ansprechend

- sehr ansprechend
 ansprechend
 wenig/nicht ansprechend

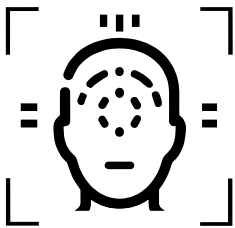
	Erkennbarkeit	Ästhetik	Gesamtpunkte Icon
Gesichtserkennung			
Icon 1	14	17	31
Icon 2	23	24	27
Icon 3	17	20	37
Biometrische Daten			
Icon 1	20	18	38
Icon 2	24	23	47
Icon 3	27	27	54
Kommunikationsüberwachung			
Icon 1	32	27	59
Icon 2	20	23	43
Icon 3	25	21	46
Gesundheitsdaten			
Icon 1	21	22	43
Icon 2	29	29	58
Icon 3	29	26	55
GPS und Standortüberwachung			
Icon 1	26	27	53
Icon 2	29	25	54
Icon 3	23	21	44
Personenbezogene Daten			
Icon 1	25	29	54
Icon 2	28	28	56
Icon 3	18	17	35
Profildaten			
Icon 1	19	17	36
Icon 2	20	20	40
Icon 3	25	26	51
Technische Daten			
Icon 1	27	27	54
Icon 2	27	23	50
Icon 3	25	25	50

Tabelle 8: Auswertung Usability-Testing Icons
Quelle: Eigene Darstellung, 2022

Bei vier der acht Auswahlmöglichkeiten fällt das Ergebnis der Auswertung sehr knapp aus und zwar in den Kategorien Gesundheitsdaten (drei Punkte Unterschied zwischen Variante 2 und 3), GPS & Standortüberwachung (ein Punkt Unterschied zwischen Variante 1 und 2), Personenbezogene Daten (zwei Punkte Unterschied zwischen Variante 1 und 2) sowie bei den Technischen Daten (Variante 1 hat vier Punkte mehr als 2 und 3).

Es wäre also denkbar, dass sich das Ergebnis in diesen Kategorien noch ändern könnte, falls weitere Personen befragt würden. Für den Übertrag in den Prototypen wird allerdings mit dem derzeitigen Resultat weitergearbeitet.

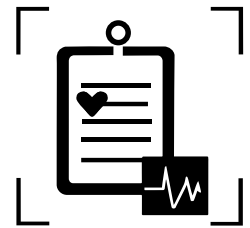
Im Folgenden sind nun die acht Icons abgebildet, die beim Testing die höchste Punktzahl erreichen.



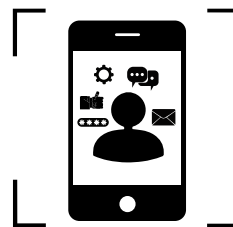
Gesichtserkennung



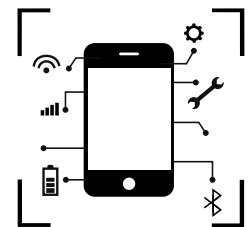
Biometrische Daten

Kommunikations-
überwachung

Gesundheitsdaten

GPS & Standort-
überwachungPersonenbezogene
Daten

Profildaten



Technische Daten

Abb. 44: Ergebnis Icon-Testing
Quelle: Eigene Darstellung, 2023



3.5 Testing Click-Dummy

Nach der finalen Festlegung der acht Icons, werden diese in den Prototypen in Figma eingefügt. Im weiteren Schritt soll durch ein Usability Testing und eine Wissensabfrage herausgefunden werden, ob die Icons ihren Zweck der Bewusstseins- und Wissensvermittlung zum Thema Datenschutz erfüllen.

3.5.1 Methodenwahl

Der Click-Dummy wird mittels induktivem Usability-Test analysiert. Diese Methode ist für Prototypen besonders gut geeignet, da dadurch Schwachstellen aufgedeckt sowie Verbesserungsmöglichkeiten gewonnen werden (Sarodnick & Brau, 2016, S. 163). Für die Evaluation wird ein Fragebogen mit insgesamt sechs Fragen erstellt - drei offene und drei geschlossene. Zwei davon zielen darauf ab, die Usability des Click-Dummies zu bewerten. Drei Fragen beziehen sich auf das Thema Datenschutz. Die Teilnehmer:innen sollen dabei mithilfe der Informationen auf den Seiten des Prototyps zu den Antworten gelangen. Die letzte Frage ist optional und für Feedback und/oder Verbesserungsvorschläge gedacht.

3.5.2 Ablauf

An dem Testing nehmen fünf Teilnehmer:innen – zwei weibliche und drei männliche – im Alter zwischen 22 und 38 Jahren teil. Die Verfasserin ist während des Testings anwesend, um bei etwaigen Schwierigkeiten im Umgang mit dem Click-Dummy behilflich sein zu können.

Alle Teilnehmer:innen beginnen auf der Startseite ohne Beschriftungen zu den Plattformen (Abb. 8, Punkt 2.4.3). Der Fragebogen wird auf einem separaten Bildschirm eingeblendet und kann während des Testings ausgefüllt werden. Für das Testing und die Beantwortung der Fragen sind jeweils zehn Minuten Zeit eingeplant, diese wird von der Verfasserin gestoppt.

Auf der folgenden Seite ist der Fragebogen abgebildet, der den Teilnehmer:innen vorgelegt wird.

Der Link zum Click-Dummy lautet wie folgt:
<https://www.figma.com/file/WO9F1C5yICr8wMHZZ70Joe/I-AGREE-to-what-I-see?type=design&node-id=5%3A2&mode=design&t=yvYr8ZzwbHdfiKDI-1>

Usability-Test Click-Dummy und Wissens- Abfrage Datenschutz - I AGREE to what I see

Link zu Prototyp auf Figma:

<https://www.figma.com/proto/WO9F1C5yICr8wMHZZ70Joe/I-AGREE-to-what-I-see?type=design&node-id=33-394&t=CTDhKbeLZorY0XiT-1&scaling=contain&page-id=5%3A2&starting-point-node-id=33%3A394&mode=design>

Befolge bitte die beschriebenen Anweisungen und beantworte anschließend die untenstehenden Fragen.

Gelange von der Startseite aus auf die Seite der von Facebook gesammelten Datenkategorien. Wie gut oder schlecht ist dir das Auffinden gelungen? Kreuze bitte jeweils eine Antwort an.

- Ich konnte es sehr leicht finden.
- Ich konnte es einigermaßen leicht finden.
- Ich konnte es kaum/gar nicht finden.

Wie (ästhetisch) ansprechend ist für dich der Aufbau der Seite?

- sehr ansprechend
- ansprechend
- wenig/nicht ansprechend

Beantworte mithilfe des Click-Dummies bitte folgende Fragen zum Thema Datenschutz:

Was zählt alles zu den biometrischen Daten?

Was sind personenbezogene Daten?

Ist die Darstellung der gesammelten Datenkategorien in Form von Icons für dich hilfreich?

- sehr hilfreich
- hilfreich
- wenig/nicht hilfreich

Hast du noch sonstige Fragen oder Anmerkungen zum Click-Dummy oder den Icons?

Vielen Dank für die Teilnahme!

3.5.3 Auswertung und Ergebnisse



Die Aufgaben können von allen fünf Teilnehmer:innen unter den vorgegebenen zehn Minuten erledigt werden. Während des Testings gibt es keine Rückfragen.

Das Auffinden der von Facebook gesammelten Datenkategorien ist für alle Teilnehmer:innen sehr leicht bzw. leicht. Auch die Ästhetik des Prototyps wird bis auf eine Ausnahme positiv bewertet. An dieser Stelle ist anzumerken, dass der Fokus des Testings hauptsächlich auf der Erkennbarkeit der Icons und dem Auffinden der Datenkategorien liegt. Eine Überarbeitung des Designs ist durchaus




denkbar. Die Darstellung der Icons wird von allen Teilnehmer:innen positiv bewertet. Beim optionalen Feedback wird zweimal angemerkt, dass diese Form der Information sehr hilfreich wäre. Eine Person gibt den Hinweis, dass der zusätzliche Text bei den Icons (Beschreibung) notwendig ist, da sie ansonsten nicht eingeordnet werden könnten.

Die Wissensfragen können von allen Teilnehmer:innen fast vollständig beantwortet werden. Weitere Testings würden mit Sicherheit zu einem aussagekräftigeren Ergebnis führen, was aus Zeitgründen bei der Fertigstellung der Arbeit allerdings nicht möglich ist.



Auffinden der Detailseite zu den von Facebook gesammelten Datenkategorien:

sehr leicht auffindbar (2x)	
leicht auffindbar (3x)	
kaum/gar nicht auffindbar	

Ästhetik Seiten-Aufbau Prototyp:

sehr ansprechend (1x)	
ansprechend (3x)	
kaum/gar nicht ansprechend (1x)	

Darstellung der Icons hilfreich?

sehr hilfreich (2x)	
hilfreich (3x)	
kaum/gar nicht hilfreich	

Interpretation und Diskussion

Befragung

Textanalyse

Cluster-Analyse

Icon-Design

Click-Dummy



4. Interpretation und Diskussion

In diesem Kapitel werden die Ergebnisse der unter Punkt 3 durchgeführten Befragungen und Testings diskutiert, um mögliche Erkenntnisse zu erlangen, die für die Beantwortung der Fragestellungen in dieser Forschungsarbeit notwendig sind. Die Punkte werden jeweils einzeln besprochen. Das Fazit zur gesamten Arbeit sowie die Beantwortung der Forschungsfragen folgen unter Punkt 5.

4.1 Befragung

Mit den zu Beginn der Arbeit durchgeführten strukturierten Interviews sollte herausgefunden werden, wie die Proband:innen ihr Verhalten im Umgang mit sozialen Medien und Messenger-Diensten einschätzen und über welches Wissen sie bezüglich Datenschutz und der Verarbeitung ihrer Daten auf diesen Plattformen verfügen.

Alle befragten Personen gaben an, mindestens eine Social-Media-Plattform und einen Messenger-Dienst regelmäßig zu nutzen. Die Privat-Nutzung von Meta lag bei 100 Prozent. Das liegt daran, dass neben Facebook und Instagram mit WhatsApp der wohl meistgenutzte Messenger-Dienst zum selben Konzern gehört.

Zwei von zehn der Befragten gaben an, schon einmal eine Datenschutzrichtlinie der untersuchten Plattformen zumindest teilweise gelesen zu haben. Allerdings mit der Anmerkung, dass dies sowohl zeitaufwändig als auch – bedingt durch die Form – mühsam war. Diese Begründung wurde auch von den Nicht-Leser:innen angegeben – zu lang/umfangreich, wenig bis gar nicht verständlich. Diese Aussagen bestätigen die zu Beginn der Arbeit aufgestellten Thesen des zu großen Umfangs und der Schwierigkeit der Texte. Zwei Personen

gaben an, dass sie sich bis dato keine Gedanken über den Inhalt der Datenschutzrichtlinien gemacht hatten, da sie diese für die Nutzung des Dienstes ohnehin akzeptieren müssten. Dieser Umstand verdeutlicht das Machtgefälle zwischen Betreibern und Nutzer:innen. Wer die Plattform nutzen möchte, muss damit leben, dass unzählige (persönliche) Daten gesammelt und auf welche Art auch immer verarbeitet werden.

Das explizite Wissen zu einzelnen gesammelten Daten ist größtenteils unzureichend. Auf die Frage, was Betreiber sozialer Medien und Messengerdienste sammeln, kam mehrmals die Aussage „alles“. Bei genauerer Nachfrage konnte dieses „Alles“ allerdings kaum genauer spezifiziert werden.

Über Nachfrage, welche Daten die Teilnehmer:innen nicht mit den Betreibern teilen möchten, waren die Antworten hingegen konkreter. So werden Gesundheitsdaten in fast allen Fällen als besonders schützenswert erachtet. Auch Informationen zum jeweiligen Gehalt, Bank- und Finanzdaten sowie Details aus dem Intim- und Privatleben möchte der Großteil der Befragten nicht auf sozialen Medien teilen. Zwei Teilnehmer:innen gaben zudem an, keine biometrischen Daten angeben zu wollen. Was ihnen bis zu diesem Zeitpunkt nicht bewusst war, ist, dass sie dies durch die Nutzung einiger sozialer Medien, die beispielsweise Gesichtserkennungstechnologie einsetzen, bereits tun.

Durch das strukturierte Interview konnten mehrere Annahmen bestätigt werden. Es hat zudem gezeigt, dass das Datenschutzbewusstsein im Allgemeinen noch stark ausbaufähig ist.

4.2 Textanalyse

Die Textanalyse der Datenschutzrichtlinien diene nicht nur der Definition der Begriffe für die Cluster-Analyse, sondern sollte auch Aufschluss über den jeweiligen Aufbau, Umfang und Inhalt geben.

Anhand der Prüfung des Lesbarkeitsindex konnte nicht nur die Schwierigkeit der Texte, sondern auch der Länge bestimmt werden. Weit voran liegt hierbei die Meta-Datenschutzrichtlinie mit 22.245 Wörtern (siehe Tabelle 2). Neben Facebook und Instagram wurden dort noch weitere Dienste des Konzerns behandelt. Die Entscheidung, alle Informationen in einer Richtlinie zusammenzufassen, lässt darauf schließen, dass Meta kein Interesse daran hat, dass diese von Nutzer:innen gelesen wird. Bei dieser Wortanzahl ist das auch sehr unwahrscheinlich. Aber auch wesentlich kürzere Texte werden nach LIX von der Komplexität her als „hoch“ bewertet. Das ist wiederum auf die sprachliche Form der Datenschutzrichtlinien zurückzuführen. Fachbegriffe, viele Wiederholungen einzelner Textpassagen sowie teilweise umständliche Formulierungen erschweren das sinnerfassende Lesen.

Interessant ist auch das Ergebnis des Messenger-Dienstes Signal. Dieser beschränkt sich nur auf die für die Funktion benötigten Daten. Mit nur 524 Wörtern fällt die Datenschutzrichtlinie vergleichsweise sehr kurz aus. Dennoch liegt der LIX bei 46.7, was eine „mittlere“ Komplexität bedeutet.

Die Begründung hierfür könnte natürlich an der Formulierung liegen, da auch dieser Text größtenteils Fachbegriffe beinhaltet. Zudem existiert die Datenschutzrichtlinie nur in englischer Sprache, was sich ebenfalls auf die Bewertung auswirken könnte.

Während des Verfassens der Arbeit wurden einige Datenschutzrichtlinien von den Betreibern aktualisiert, es gilt also immer das oben angegebene Datum. In dieser Zeit erfolgte auch die Gründung des Meta-Konzerns. Zuvor verfügte sowohl Facebook als auch Instagram über eine eigene Datenschutzrichtlinie. Bei der Textanalyse konnte hierbei eine interessante Entdeckung gemacht werden. In der Instagram-Datenschutzrichtlinie aus dem Jahr 2020 wird beispielsweise explizit der Einsatz von Gesichtserkennungstechnologie erwähnt (siehe Abb. 46). Diese gehört ja zu den biometrischen Daten und gilt laut DSGVO als besonders schützenswert (EU Verordnung 2016/679). In der aktuellen Richtlinie von Meta wird diese allerdings an keiner Stelle direkt oder indirekt erwähnt. Nachdem das Markieren und Erkennen von Personen auf Bildern aber nach wie vor möglich ist, kann ausgeschlossen werden, dass der Konzern diese Technologie nicht mehr einsetzt. Die Frage, die sich diesbezüglich eher stellt ist, ob das Weglassen dieser durchaus wichtigen Information in Ordnung ist.

Da die Datenschutzrichtlinien aber großteils nicht gelesen werden, wird dieses Detail kaum jemandem auffallen.

Gesichtserkennung: Wenn du dies aktiviert hast, nutzen wir Gesichtserkennungstechnologie, um dich auf Fotos bzw. in Videos und Kameraerlebnissen wiederzuerkennen. Bei den von uns erstellten Gesichtserkennungsvorlagen handelt es sich gemäß EU-Recht um Daten mit besonderem Schutz. Erfahre mehr darüber, wie wir Gesichtserkennungstechnologie

4.3 Cluster-Analyse

Anhand der Cluster-Analyse ließen sich vier große Gruppierungen identifizieren, die folgendermaßen zusammengefasst werden können:

- Cluster 1: Profildaten
- Cluster 2: Personenbezogene bzw. besonders schützenswerte Daten
- Cluster 3: Demografische bzw. personenbezogene Daten
- Cluster 4: Technische Daten

Der erste Cluster beinhaltet vor allem Informationen, die mit einer aktiven Interaktion der Nutzer:innen verbunden sind. Für die Bezeichnung dieser Kategorie wählten die Teilnehmer:innen des Cardsortings häufig Begriffe wie Profildaten, Plattformdaten, User-Aktion, User-Interaktion, Nutzungsdaten sowie Verhaltensbezogene Daten. Das zeigt, dass Kompetenz im Umgang mit den sozialen Medien bei den Nutzer:innen auf jeden Fall vorhanden ist.

Im zweiten Cluster wurden einige Daten gruppiert, die keine Aktivität der Nutzer:innen voraussetzen. Darin finden sich auch fast alle Daten, die laut Artikel 9 DSGVO als besonders schützenswert gelten (EU Verordnung 2016/679). Diese wurden im Cardsorting unter anderem als persönliche, sensible, höchstpersönliche, geheime sowie empfindliche Daten bezeichnet. Das zeigt, dass Nutzer:innen der Wert dieser Daten durchaus bewusst zu sein scheint. Aktiv würden sie diese in den wenigsten Fällen angeben. Allerdings scheint einigen Proband:innen nicht klar zu sein, dass sich gewisse Informationen auch indirekt aus den Datensätzen herauslesen lassen.

Cluster 3 enthält, wie weiter oben erwähnt, vor allem demografische und in diesem Sinn, personenbezogene Daten. Dass die ethnische Herkunft, die ebenfalls zu Artikel 9 DSGVO ge-

hört, diesem Cluster zugeordnet wurde, zeigt, dass Nutzer:innen die besonders schützenswerten Daten nicht zu kennen scheinen und diese Information möglicherweise als weniger relevant einschätzen. Diese Kategorie wurde von den Teilnehmer:innen als persönliche, allgemeine, Anschrift-, Kontakt-, Identitäts- und personenbezogene Daten bezeichnet.

Der vierte Cluster umfasst großteils technische, aber auch Tracking-Daten wie GPS, Geo-Tag und IP-Adresse. Dementsprechend wurden auch die Kategorien von den Teilnehmer:innen benannt: Technische Daten, Technik-Daten, Geräte-Daten, Überwachungsdaten, Mobildaten, Standortdaten und Bewegungsdaten. Obwohl die IP-Adresse zu den personenbezogenen Daten gehört, da durch sie eine Person identifizierbar sein kann, wird sie der Technik zugeordnet. Das ist grundsätzlich nachvollziehbar, zeigt aber auch, dass den Nutzer:innen häufig das Hintergrundwissen zu gewissen Informationen und vor allem zum Datenschutz fehlt.



4.4 Icon-Design

Das informationsgrafische Zeichensystem bildet den eigentlichen Kern dieser Forschungsarbeit, da es von wesentlicher Bedeutung für die Beantwortung der Fragestellungen ist.

Die insgesamt acht Kategorien wurden von dem Ergebnis der Cluster-Analyse abgeleitet und teilweise zusammengefasst. Da beispielsweise die IP-Adresse von den Teilnehmer:innen des Cardsortings meistens den technischen Daten zugeordnet wurde, ist dies auch in den Icon-Kategorien übernommen worden, allerdings mit einer entsprechenden Erklärung.

Das Testing der Icons hat zu einem überwiegend positiven Ergebnis geführt. Die meisten davon waren für die Teilnehmer:innen sehr gut bis gut erkennbar. Es gilt zu beachten, dass die Icons nicht völlig isoliert, also ohne Angabe der Datenkategorie, getestet wurden. Es ist anzunehmen, dass die Erkennbarkeit ohne den entsprechenden Kontext geringer ausgefallen wäre. Da die Bezeichnung aus Datenschuttsicht allerdings genauso relevant ist, kann dieser Fakt vernachlässigt werden.

Bei einigen Icons ist das Ergebnis recht knapp ausgefallen (siehe Tabelle 8). Es wäre also durchaus interessant, ob und wie sich das Resultat durch eine Erhöhung der Anzahl von Testpersonen verändern würde. Die Kategorie der Gesichtserkennung erzielte im Vergleich eine deutlich geringere Punktezahl. Daraus lässt sich ableiten, dass möglicherweise keine der drei Varianten ideal umgesetzt wurde und somit eine Überarbeitung notwendig wäre.

Eine der zwölf Testpersonen hat alle Varianten sehr gering bewertet. Dieser Bewertung sollte allerdings nicht zu viel Gewicht beigegeben werden, da das Ergebnis ansonsten vergleichsweise sehr gut ausgefallen ist. Es legt allerdings nahe, dass nicht alle Nutzer:in-

nen mit dem Umgang mit Icons vertraut sind oder – aufgrund ihrer Wahrnehmung – keine Informationen aus dieser Darstellungsform ziehen können.

4.5 Click-Dummy

Der Prototyp wurde im Allgemeinen recht positiv bewertet. Aufgrund der geringen Anzahl an Testpersonen ist das Ergebnis allerdings nicht sehr aussagekräftig. Hier müssten auf jeden Fall weitere Überprüfungen stattfinden. Einen kleinen Einblick lässt das Ergebnis aber dennoch zu.

Obwohl der Aufbau des Prototypens noch recht einfach ist, war das Feedback zum Umgang und der Ästhetik überwiegend positiv. Insbesondere die Bewertung des Einsatzes der Icons gilt es hier hervorzuheben, da dieser überwiegend als hilfreich eingestuft wurden. Das ließ sich auch am Feedback von drei Testpersonen ableiten, die den Einsatz von Icons als Überblick der gesammelten Daten durchaus positiv einstufen würden.

Da der Click-Dummy vorwiegend der Überprüfung des Zeichensystems diente, müsste die Usability im Allgemeinen auf jeden Fall ausführlicher getestet werden.

Conclusio und Ausblick

5. Conclusio und Ausblick

Die vorliegende Forschungsarbeit verfolgte das Ziel, herauszufinden, inwieweit Zeichen bei der Vermittlung eines Datenschutzbewusstseins bzw. den Inhalten von Datenschutzrichtlinien sozialer Medien und Messenger-Dienste förderlich sein können.

Die Ergebnisse der durchgeführten Analysen legen nahe, dass Informations-Design durchaus hilfreich bei der Vermittlung von Datenschutzhinhalten ist. Das entwickelte Zeichensystem ermöglicht es den Nutzer:innen, einen schnellen Überblick der gesammelten Daten zu erlangen. Um zu prüfen, wie nachhaltig diese Wissensvermittlung ist, könnten die Zeichen im Rahmen von Schulungen zur Medien- bzw. Datenkompetenz eingesetzt werden.

Es ist wahrscheinlich, dass die Datenschutzrichtlinien auch zukünftig so gut wie nie gelesen werden und der „I AGREE“-Button ohne weitere Bedenken gedrückt wird. Eine Reduktion der Inhalte wäre auf jeden Fall hilfreich, es ist allerdings davon auszugehen, dass die Anbieter weiterhin kein Interesse daran haben, Nutzer:innen diese Information in kurzer, gut verständlicher Form darzulegen. Den Anbietern von Twitter scheint dieser Umstand zumindest bewusst zu sein. Das legt der Einstieg ihrer Datenschutzrichtlinie nahe: „Es ist wirklich schwer, alle mit einer Datenschutzerklärung zufrieden zu stellen. [...] Wir wünschen zwar, wir könnten alles, was Sie wissen müssen, in einen Tweet packen [...]“ (Twitter - Datenschutzrichtlinie, 2023).


Alle relevanten Informationen in einem Tweet unterzubringen ist nicht notwendig. Es wäre schon ausreichend, Nutzer:innen über die wichtigsten Verarbeitungen ihrer Daten zu informieren. Es ist allerdings nicht davon auszugehen, dass dies in naher Zukunft passieren wird. Die „Gleichheit der informatiellen Ver-

hältnisse zwischen Anbietern der Innovationen und Nutzern“ (Müller, 2020, S. 525) ist nicht gegeben. Zudem scheint der Wille zur Nutzung der Plattformen bei vielen Nutzer:innen größer zu sein, als datenschutzrechtliche Bedenken und damit verbundene Risiken.

Die Reduktion der relevanten Inhalte von Datenschutzrichtlinien auf Icons hat aber durchaus gezeigt, dass sie diese zugänglicher machen würden. Insbesondere, wenn es darum geht, sich rasch einen Überblick zu verschaffen. Der „I AGREE“-Button würde dadurch sicherlich nicht weniger häufig gedrückt werden. Allerdings würden die Nutzer:innen dadurch zumindest über ein Grundwissen zu den verarbeiteten Daten und eingesetzten Technologien verfügen.

Mit den in dieser Arbeit entwickelten Icons konnte zumindest ansatzweise belegt werden, dass sich diese Form der Informationsvermittlung von Datenschutzhinhalten durchaus eignen kann. Da Zeichen immer mit vorhandenem Wissen verknüpft und erlernt werden müssen, sollte die Vermittlung dieser Kompetenzen schon möglichst früh, beispielsweise in der Grundschule, beginnen.

Gerade im Hinblick auf neue Technologien und dem zunehmenden Einsatz von künstlicher Intelligenz wird es immer wichtiger, über ein entsprechendes Datenschutzbewusstsein zu verfügen. Neben zahlreicher positiver Entwicklungen fördern diese Innovationen auch die Möglichkeiten des Datenmissbrauchs und der Manipulation. Die Akzeptanz und der Umgang mit diesen ist bei vielen Nutzer:innen vorhanden. Das zeigt sich auch am Beispiel der sozialen Medien. Die Nutzung sowie das Erzeugen und Teilen von Inhalten ist für Menschen jeder Altersklasse und unabhängig vom Bildungsgrad ohne weiteres möglich. Werden



sie allerdings mit inhaltlichen Fragen, beispielsweise zu Funktion oder mit Datensätzen verbundenen Risiken (z. B. Gesichtserkennung) konfrontiert, treten deutliche Wissensdefizite zu Tage.

Fakt ist auch, dass der Datenschutz der Technik deutlich hinterher hinkt. Die Entwicklung von der Datenschutzrichtlinie 1995 (Richtlinie 95/46/EG) des Europäischen Parlaments bis zur Datenschutzgrundverordnung (EU Verordnung 2016/679) dauerte über 20 Jahre. Hier gilt es zu bedenken, dass diese Zeitspanne von zahlreichen digitalen Innovationen geprägt war. Eine Zeit, in der auch die sozialen Medien und Messenger-Dienste entstanden sind.

Es stellt sich also die Frage, ob die technischen Gegebenheiten und datengetriebenen Technologien neue Datenschutzkonzepte erfordern würden, die es ermöglichen, unmittelbar auf Veränderungen reagieren zu können. Nutzer:innen sollten ihre Datensouveränität zurückerlangen, aber gleichzeitig auch mehr Verantwortung für ihre eigenen Daten übernehmen.

Ob dieser Schritt in naher Zukunft überhaupt möglich sein wird, hängt auch stark von der Medienkompetenz der Nutzer:innen ab. In diesem Bereich besteht deutlicher Handlungsbedarf. Aufgrund der erarbeiteten Ergebnisse konnte allerdings festgestellt werden, dass Design, insbesondere mit menschenzentriertem Ansatz, einen wertvollen Beitrag zur Förderung der (Datenschutz-)Kompetenz, des Datenschutzbewusstseins und der Informationsvermittlung leisten kann.

Bezogen auf die Inhalte und Ergebnisse schließt diese Forschungsarbeit mit folgendem, leicht abgeänderten Sprichwort:

Ein Icon sagt manchmal mehr als tausend Worte.

***„Above all else
show the data.”***

Edward Tufte, 1983, S.105

Literaturverzeichnis

Literaturverzeichnis

Klumpp, D. (2020). Digitalordnung: Privacy by Design, by Default oder per Datensouveränität? In Hentschel, A., Hornung, G., & Jandt, S. (Hrsg.), *Mensch – Technik – Umwelt: Verantwortung für eine sozialverträgliche Zukunft* (S. 509-523), 1. Auflage. Baden-Baden: Nomos Verlagsgesellschaft.

Müller, G. (2020). Verhindert das Privatheitsparadox modernen Datenschutz? In Hentschel, A., Hornung, G., & Jandt, S. (Hrsg.), *Mensch – Technik – Umwelt: Verantwortung für eine sozialverträgliche Zukunft* (S. 525-543), 1. Auflage. Baden-Baden: Nomos Verlagsgesellschaft.

Christian, A. (2017). *Piktogramme – Tendenzen in der Gestaltung und im Einsatz grafischer Symbole*. Köln: Herbert von Halem Verlag.

Sarodnick, F., & Brau, H. (2016). *Methoden der Usability Evaluation: Wissenschaftliche Grundlagen und praktische Anwendung*, 3., unveränderte Auflage. Bern: Hogrefe AG.

Kirk, A. (2016). *Data Visualisation – A Handbook for Data Driven Design*. Los Angeles, London, New Delhi, Singapore, Washington DC, Melbourne: SAGE Publications Ltd.

Götz, V., & Rigamonti, A. (2015). *Informationsvisualisierung – Missbrauch und Möglichkeit*. Stuttgart: av edition.

Schnell, R., Hill, P. B., & Esser, E. (2008). *Methoden der empirischen Sozialforschung*, 8., unveränderte Auflage. München/Wien: Oldenburg Verlag.

Krampen, M., Götte, M., & Kneidl, M. (2007). *Die Welt der Zeichen – Kommunikation mit Piktogrammen*. Ludwigsburg: av edition.

Hartmann, F., & Bauer, E. K. (2006). *Bildsprache – Otto Neurath Visualisierungen*, 2. erweiterte und durchgesehene Auflage. Wien: Facultas Verlags- und Buchhandels AG WUV.

Maeda, J. (2006). *The Laws of Simplicity – Design, Technology, Business, Life*. Cambridge (Massachusetts): MIT Press.

Nöth, W. (2000). *Handbuch der Semiotik*, 2., vollständig neu bearbeitete und erweiterte Auflage. Stuttgart: Metzlersche Verlagsbuchhandlung.

Frutiger, A. (1998). *Der Mensch und seine Zeichen*, 6. Auflage. Wiesbaden: Fourier Verlag GmbH.

Aicher, O., & Krampen, M. (1996). *Zeichensysteme der visuellen Kommunikation*, Neuausgabe 1996. Stuttgart: Ernst und Sohn Verlag für Architektur.

Tufte, E. (1990). *Envisioning Information*. Connecticut: Graphics Press.

Anderson, J. R. (1988). *Kognitive Psychologie – Eine Einführung*. Heidelberg: Spektrum Verlag.

Tufte, E. (1983). *The Visual Display of Quantitative Information*. Connecticut: Graphics Press.



Gibson, J. J. (1982). *Wahrnehmung und Umwelt – Der ökologische Ansatz in der visuellen Wahrnehmung*. München, Wien, Baltimore: Urban & Schwarzenberg.

Bertin, J. (1974). *Graphische Semiologie – Diagramme, Netze, Karten*, 2. Auflage. Berlin: De Gruyter.

Kennedy, J. M. (1974). *A Psychology of Picture Perception – Images and Information*. San Francisco: Jossey-Bass, Inc., Publishers.

Bentham, J. (1787: Panoptikum oder Das Kontrollhaus. In Welzenbacher, Ch. (Hrsg., 2013), *Das Panoptikum*. Berlin: Matthes & Seitz.

Online:

Bundesamt für Sicherheit in der Informationstechnik (2023). *Spam, Phishing & Co – So erkennen Sie gefälschte und schadhafte E-Mails*. URL: <https://www.bsi.bund.de/dok/6696702> [letzter Zugriff am 25.06.2023]

Der Standard (2023). *Private Daten von mehr als 200 Millionen Twitter-Nutzern kursieren kostenlos im Internet*. URL: <https://www.derstandard.at/story/2000142324523/private-daten-von-mehr-als-200-millionen-twitter-nutzern-kursieren> [letzter Zugriff am 25.06.2023]

Meta (2023). *Facebook und Instagram Datenschutzrichtlinie*. URL: <https://de-de.facebook.com/privacy/policy> [letzter Zugriff am 12.01.2023]

None of your business (2023). *Meta darf personenbezogene Daten nicht für Werbung nutzen*. URL: <https://noyb.eu/de/breaking-meta-darf-personenbezogene-daten-nicht-fuer-werbung-nutzen> [letzter Zugriff 06.02.2022]

Posit – The Open-Source Data (2023). *The RStudio Desktop*. URL: <https://posit.co/download/rstudio-desktop/>

Collaud, R., Reppa, I., Défayes, L., McDougall, S., Henchoz, N., & Sonderegger, A. (2022). *Design standards for icons: The independent role of aesthetics, visual complexity and concreteness in icon design and icon understanding*. *Displays*, Volume 74, September 2022, Nr. 102290. URL: <https://www.sciencedirect.com/science/article/pii/S0141938222001093>

LinkedIn (2022). *Über LinkedIn*. URL: https://about.linkedin.com/de-de?trk=content_footer_about&lr=1 [letzter Zugriff am 06.02.2022]

Meta (2022). *About Meta/Facebook*. URL: https://about.facebook.com/company-info/?_ga=2.74563286.513956802.1643990628-907250016.1643990628 [letzter Zugriff am 06.02.2022]

Meta (2022). *Whatsapp Datenschutzrichtlinie*. URL: <https://www.whatsapp.com/legal/privacy-policy-eea> [letzter Zugriff am 06.02.2022]

Statista Research Department (2022). Anzahl der monatlich aktiven Facebook Nutzer weltweit vom 1. Quartal 2009 bis zum 4. Quartal 2021. URL: <https://de.statista.com/statistik/daten/studie/37545/umfrage/anzahl-der-aktiven-nutzer-von-facebook/> [letzter Zugriff am 06.02.2022]

Süddeutsche Zeitung (2022): Whistleblower kritisiert Twitter-Management scharf. URL: <https://www.sueddeutsche.de/politik/datenschutz-whistleblower-kritisiert-twitter-management-scharf-dpa.urn-newsml-dpa-com-20090101-220913-99-747070> [letzter Zugriff am 25.06.2023]

Tagesschau (2022). Musk schließt Twitter-Kauf ab, Mit Informationen von Nils Dampz, ARD-Studio Los Angeles. URL: <https://www.tagesschau.de/wirtschaft/twitter-kauf-musk-abschluss-101.html> [letzter Zugriff am 25.06.2023]

TikTok (2022). TikTok Datenschutzerklärung. URL: <https://www.tiktok.com/legal/privacy-policy-eea?lang=de> [letzter Zugriff am 06.02.2022]

Twitter (2022). Datenschutzerklärung. URL: <https://twitter.com/de/privacy> [letzter Zugriff am 06.02.2022]

FAZ (2021). Hacker bieten Daten zu 700 Millionen LinkedIn-Nutzern an. In: Frankfurter Allgemeine Zeitung FAZ.NET. URL: <https://www.faz.net/aktuell/wirtschaft/digitec/linkedin-hacker-besitzen-angeblich-daten-zu-700-millionennutzern-17412479.html> [letzter Zugriff am 06.02.2022]

Köver, Ch. (2021). TikTok verschärft Datenschutz-Einstellungen für Jugendliche. In: Netzpolitik. Org. URL: <https://netzpolitik.org/2021/reaktion-auf-politischen-druck-tiktok-verschaerft-datenschutz-einstellungen-fuer-jugendliche/> [letzter Zugriff am 06.02.2022]


Meta (2021). Tech at Meta – Connect 2021: Our vision vor the metaverse. URL: <https://tech.facebook.com/reality-labs/2021/10/connect-2021-our-vision-for-the-metaverse/>

Verbraucherzentrale NRW.ev (2021). Datenlecks bei Facebook: So prüfen Nutzer, ob sie betroffen sind. URL: <https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/datenlecks-bei-facebook-so-pruefen-nutzer-ob-sie-betroffensind-25013> [letzter Zugriff am 06.02.2022]

Zeit Online (2021). WhatsApp-Konkurrenten verzeichnen starken Nutzeranstieg. URL: <https://www.zeit.de/digital/datenschutz/2021-01/messengerdienste-whatsapp-konkurrenz-starker-nutzeranstieg-threema-telegram-signal-datenschutz> [letzter Zugriff am 25.06.2023]

Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (2020). Corona-Ampel. URL: <https://corona-ampel.gv.at> [letzter Zugriff am 25.06.2023]

LinkedIn (2020). LinkedIn Datenschutzerklärung. URL: <https://de.linkedin.com/legal/privacy-policy> [letzter Zugriff am 06.02.2022]



Sinnig, C. (2020). Informationsarchitektur meistern: 3 Card-Sorting-Methoden für eine bessere Navigation. Userlutions, Usability-Analyse. URL: <https://userlutions.com/blog/usability-analyse/card-sorting-informationsarchitektur/>

Dachwitz, I., Rudl, T., & Rebiger, S. (2018). Was wir über den Skandal um Facebook und Cambridge Analytica wissen. In: Netzpolitik.Org. URL: <https://netzpolitik.org/2018/cambridge-analytica-was-wir-ueber-das-groesste-datenleck-in-der-geschichte-von-facebook-wissen/> [letzter Zugriff am 06.02.2022]

Obar, J. A., & Oeldorf-Hirsch, A. (2018). The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services, *Information, Communication & Society*, 23:1, 128-147. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465 [letzter Zugriff am 25.06.2023]

Signal Org. (2018). Signal Privacy Policy. URL: <https://signal.org/legal/#privacy-policy> [letzter Zugriff am 06.02.2022]

BGBl. I Nr. 120/2017, Bundeskanzleramt (2017). Datenschutzanpassungsgesetz 2018, Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (Datenschutz-Anpassungsgesetz 2018). URL: <https://www.ris.bka.gv.at/eli/bgbl/i/2017/120> [letzter Zugriff am 06.02.2023]

Cakebread, C. (2017). You're not alone, no one reads terms of service agreements. In: *Business Insider*. URL: <https://www.businessinsider.in/Youre-not-alone-no-one-reads-terms-of-service-agreements/articleshow/61659553.cms> [letzter Zugriff am 06.02.2022]

Lenhard, A., & Lenhard, W. (2017). *Psychometrica – Lesbarkeitsindex*. URL: <https://www.psychometrica.de/lix.html>

Harley, A. (2016). Usability Testing of Icons. Nielsen Norman Group. URL: <https://www.nngroup.com/articles/icon-testing/>

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). URL: <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016R0679> [letzter Zugriff am 06.02.2022]

83. Bundesgesetz (ausgegeben am 23.5.2013), mit dem das Datenschutzgesetz 2000 geändert wird (DSG-Novelle 2014). URL: https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2013_I_83/BGBLA_2013_I_83.pdf [letzter Zugriff am 06.02.2022]

Cashmore, P. (2009). Privacy is dead, and social media hold smoking gun. In: *Special to CNN*, 28.10.2009. URL: <https://edition.cnn.com/2009/OPINION/10/28/cashmore.online.privacy/> [letzter Zugriff am 02.06.2023]

Spektrum.de (1999). Lexikon der Biologie – Reiz. In: Spektrum Akademischer Verlag. URL: <https://www.spektrum.de/lexikon/biologie/reiz/56139#> [letzter Zugriff am 25.06.2023]

Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. EUR-Lex. URL: <https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A31995L0046> [letzter Zugriff am 06.02.2022]

565 Bundesgesetz: Datenschutzgesetz DSG1978 über den Schutz personenbezogener Daten, Wien. URL: https://www.ris.bka.gv.at/Dokumente/BgblPdf/1978_565_0/1978_565_0.pdf [letzter Zugriff am 06.02.2022]

Wittgenstein, L. (1922). Tractatus Logico-Philosophicus. In The Wittgenstein Project (2022), Logisch-philosophische Abhandlung, digitale Ausgabe von Ludwig Wittgensteins Tractatus Logico-Philosophicus, Hrsg. Ogden, C. K., Ramsey, F. P., Kegan, P., & Trench, Trubner & Co. (1922). URL: https://www.wittgensteinproject.org/w/index.php/Logisch-philosophische_Abhandlung

Dudenredaktion. (o. D.). Konnotativ. In Duden online. URL: <https://www.duden.de/rechtschreibung/konnotativ>

Dudenredaktion. (o. D.). Denotat. In Duden online. URL: <https://www.duden.de/rechtschreibung/Denotat> [letzter Zugriff 06.02.2022]

Wikipedia. (o. D.). Hashtag. URL: <https://de.wikipedia.org/wiki/Hashtag> [letzter Zugriff am 02.06.2023]

Wikipedia. (o. D.). Twitter. URL: <https://de.wikipedia.org/wiki/Twitter#:~:text=Geschichte,-Siehe%20auch%3A%20Twitter&text=Twitter%20wurde%20im%20M%C3%A4rz%202006,just%20setting%20up%20my%20twtr> [letzter Zugriff am 02.06.2023]


Quelle Logos:

LinkedIn (o. D.). Logo LinkedIn. URL: <https://brand.linkedin.com/downloads> [letzter Zugriff am 02.06.2023]

Meta (o. D.). Logo Facebook. URL: <https://about.meta.com/de/brand/resources/facebookapp/logo/> [letzter Zugriff am 02.06.2023]

Meta (o. D.). Logo Instagram. URL: <https://about.meta.com/de/brand/resources/instagram/instagram-brand/> [letzter Zugriff am 02.06.2023]

Meta (o. D.). Logo WhatsApp. URL: <https://about.meta.com/de/brand/resources/whatsapp/whatsapp-brand/> [letzter Zugriff am 02.06.2023]



TikTok (o. D.). Logo TikTok. URL: https://developers.tiktok.com/doc/getting-started-design-guidelines?enter_method=left_navigation [letzter Zugriff am 02.06.2023]

Twitter (o. D.). Logo Twitter. URL: <https://about.twitter.com/en/who-we-are/brand-toolkit> [letzter Zugriff am 02.06.2023]

Eidesstattliche Erklärung

Ich erkläre hiermit an Eides statt, dass ich die vorliegende Masterarbeit selbstständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Stellen sind als solche kenntlich gemacht.

Die Arbeit wurde bisher weder in gleicher noch in ähnlicher Form einer anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Dornbirn, am 04. Juli, 2023

Anhang

01 Fragebögen soziale Medien

02 Textanalyse

03 Cardsorting und Cluster-Analyse

04 Icon-Präferenz-Testing

05 Prototyp und Auswertung



Fragebogen Nutzung sozialer Medien

Einführung/Erklärung: In dieser Befragung geht es um dein Nutzungsverhalten von sozialen Medien und Messenger-Diensten sowie um deinen Wissensstand zum Thema Datenschutz in diesem Bezug. Antworte bitte spontan auf die Fragen - es gibt kein Richtig oder Falsch.

Hinweis: Die von dir angegebenen Daten und Antworten lassen keine Rückschlüsse auf deine Person zu. Die Verarbeitung erfolgt ausschließlich zum Zweck dieses Forschungsprojekts.

Personen-Kennung: ID1

Alter: 36

Geschlecht: weiblich
 männlich

1. Nutzt du soziale Medien und/oder Messenger-Dienste?

privat: JA NEIN
beruflich: JA NEIN

2. Welche sozialen Medien und Messenger-Dienste nutzt du?

privat: früher Facebook, mittlerweile Account gelöscht, Whatsapp, Twitter, Signal, Microsoft Teams und YouTube

beruflich: Microsoft Teams

3. Welche Daten musstest du bei der Anmeldung bei den jeweiligen Plattformen/ Diensten angeben?

Meistens E-Mail-Adresse, Name, Geburtsdatum, Telefonnummer, Passwort, Geschlecht

4. Hast du dir die Datenschutzrichtlinie der jeweiligen Plattform / des jeweiligen Dienstes durchgelesen?

JA
 NEIN

5. Wenn JA / NEIN, warum?

Nein, hätte ich sie gelesen, wäre ich wahrscheinlich nicht Mitglied des Dienstes geworden, da ich die generelle Datenerhebung erschreckend finde. Umgekehrt habe ich Funktionen wie Archivierung / Wiederherstellung von WhatsApp Nachrichten sowie das automatische Downloaden von Bildern und Videos deaktiviert.

6. Was glaubst du, welche Daten die jeweiligen Unternehmen von dir sammeln?

Suchverläufe, Onlinezeit, eigene Kontakte, Bilder, Daten aus den Nachrichten, Bewegungsdiagramm, Ortsfunktion und sicher noch sehr viel mehr.

7. Siehst du darin irgendwelche Gefahren oder Risiken für dich?

In WhatsApp sehe ich ein notwendiges Übel, aber Facebook empfand ich zunehmend als Gefahr mit der Funktion auf Fotos verlinkt werden, voller Name, am besten noch mit Angaben zum Beruf und alles.

8. Gibt es Informationen, die du lieber nicht mit diesen Unternehmen teilen möchtest?

Bankdaten, Impfstatus, Gesundheitsdaten, biometrische Daten, politische Einstellung- ich finde, das geht einfach niemanden etwas an.

9. Wäre ein Leben ohne soziale Medien und Messenger-Dienste für dich vorstellbar?

- JA
- NEIN

10. Wenn JA / NEIN, warum?

Also auf soziale Medien könnte ich eher verzichten als auf Messenger-Dienste. Die meiste Kommunikation mit meiner Familie und meinen Freunden findet dort statt. Auf YouTube würde ich auch nicht gerne verzichten. Da ich dort nur konsumiere, ist es mir egal. Meinen Musikverlauf können sie ruhig tracken.

Vielen Dank für das Gespräch!

Fragebogen Nutzung sozialer Medien

Einführung/Erklärung: In dieser Befragung geht es um dein Nutzungsverhalten von sozialen Medien und Messenger-Diensten sowie um deinen Wissensstand zum Thema Datenschutz in diesem Bezug. Antworte bitte spontan auf die Fragen - es gibt kein Richtig oder Falsch.

Hinweis: Die von dir angegebenen Daten und Antworten lassen keine Rückschlüsse auf deine Person zu. Die Verarbeitung erfolgt ausschließlich zum Zweck dieses Forschungsprojekts.

Personen-Kennung: ID2

Alter: 35

Geschlecht: weiblich
 männlich

1. Nutzt du soziale Medien und/oder Messenger-Dienste?

privat: JA NEIN
beruflich: JA NEIN

2. Welche sozialen Medien und Messenger-Dienste nutzt du?

privat: Ich nutze Instagram, bin aber nicht wirklich aktiv. Ansonsten verwende ich Signal, YouTube und Skype. WhatsApp und Facebook habe ich gelöscht. Da ich mein Firmen-Handy privat verwende, durfte ich WhatsApp nicht mehr nutzen.

beruflich: Hauptsächlich Teams und LinkedIn. Das benötige ich vor allem für die Kommunikation mit Kund:innen.

3. Welche Daten musstest du bei der Anmeldung bei den jeweiligen Plattformen/ Diensten angeben?

Ich glaub meinen Namen, E-Mail-Adresse, Nutzer-Namen, Wohnort, Geschlecht. Manchmal Telefonnummer, Profilbild und auf LinkedIn Beruf und Ausbildung.

4. Hast du dir die Datenschutzrichtlinie der jeweiligen Plattform / des jeweiligen Dienstes durchgelesen?

JA
 NEIN

5. Wenn JA / NEIN, warum?

Also zumindest teilweise. Komplett habe ich mir das noch nie durchgelesen, das ist einfach viel zu viel.

6. Was glaubst du, welche Daten die jeweiligen Unternehmen von dir sammeln?

Alles? Zumindest alles, was sie kriegen können. Persönliche Daten, Bewegungsdaten, was ich mir so ansehe und was ich auf der Plattform mache, sicher auch mein Kaufverhalten usw.

7. Siehst du darin irgendwelche Gefahren oder Risiken für dich?

Auf jeden Fall. Gewisse Dinge sind einfach nicht für die Öffentlichkeit bestimmt und das soll auch so bleiben. Privatsphäre bedeutet für mich ein Stück Freiheit.

8. Gibt es Informationen, die du lieber nicht mit diesen Unternehmen teilen möchtest?

Auf jeden Fall! Beispielsweise meine Gesundheitsdaten, Gehalt, sexuelle Orientierung, private Nachrichten. Aber auch meine ganzen Aktivitäten in der Freizeit. Die gehen einfach nicht jeden etwas an. In beruflicher Hinsicht natürlich geplante Projekte und die Kommunikation darüber.

9. Wäre ein Leben ohne soziale Medien und Messenger-Dienste für dich vorstellbar?

- JA
 NEIN

10. Wenn JA / NEIN, warum?

Soziale Medien an sich wären mir eher egal, weil ich selbst nicht wirklich aktiv bin - zumindest privat. Außer natürlich LinkedIn, das geht beruflich leider nicht anders. Signal finde ich ok und ansonsten greife ich generell lieber mal zum Telefon und ruf die Leute direkt an.

Vielen Dank für das Gespräch!

Fragebogen Nutzung sozialer Medien

Einführung/Erklärung: In dieser Befragung geht es um dein Nutzungsverhalten von sozialen Medien und Messenger-Diensten sowie um deinen Wissensstand zum Thema Datenschutz in diesem Bezug. Antworte bitte spontan auf die Fragen - es gibt kein Richtig oder Falsch.

Hinweis: Die von dir angegebenen Daten und Antworten lassen keine Rückschlüsse auf deine Person zu. Die Verarbeitung erfolgt ausschließlich zum Zweck dieses Forschungsprojekts.

Personen-Kennung: ID3

Alter:

Geschlecht: weiblich
 männlich

1. Nutzt du soziale Medien und/oder Messenger-Dienste?

privat: JA NEIN
beruflich: JA NEIN

2. Welche sozialen Medien und Messenger-Dienste nutzt du?

privat: Instagram, Pinterest, WhatsApp, YouTube, Facebook

beruflich: LinkedIn, MS Teams

3. Welche Daten musstest du bei der Anmeldung bei den jeweiligen Plattformen/ Diensten angeben?

Meinen Namen, Wohnort glaube ich, E-Mail-Adresse und je nachdem einen Profil-Namen, Interessen usw.

4. Hast du dir die Datenschutzrichtlinie der jeweiligen Plattform / des jeweiligen Dienstes durchgelesen?

JA
 NEIN

5. Wenn JA / NEIN, warum?

Naja, die sind halt ziemlich lang. Ich kann mir schon vorstellen, dass da wichtige Sachen drinstehen, aber wer hat schon Zeit und Lust, das alles zu lesen. Wenn ich es nutzen will, hab ich eigentlich eh keine andere Wahl.

6. Was glaubst du, welche Daten die jeweiligen Unternehmen von dir sammeln?

Ja auf jeden Fall die Daten, die ich angegeben habe. Ansonsten denke ich mal meine Interaktionen, Kommentare, die ich hinterlasse, eventuell auch Freundeslisten.

7. Siehst du darin irgendwelche Gefahren oder Risiken für dich?

Nein, eigentlich nicht. Ich teile ja keine wirklich privaten Dinge. Damit können die ja nichts machen.

8. Gibt es Informationen, die du lieber nicht mit diesen Unternehmen teilen möchtest?

Also meine Krankenakte würde ich jetzt nicht gerne mit jedem Teilen - das gilt natürlich auch für die meiner Kinder. Naja und die Bilder von manchen Feiern auch nicht, aber die werden in meinem Freundeskreis auch nicht geteilt.

9. Wäre ein Leben ohne soziale Medien und Messenger-Dienste für dich vorstellbar?

- JA
- NEIN

10. Wenn JA / NEIN, warum?

Die komplette Kommunikation mit meiner Familie und Freunden läuft eigentlich über WhatsApp. Ich telefoniere kaum. Auf Instagram könnte ich eher verzichten, aber da sehe ich im Moment auch keinen Grund dafür.

Vielen Dank für das Gespräch!

Fragebogen Nutzung sozialer Medien

Einführung/Erklärung: In dieser Befragung geht es um dein Nutzungsverhalten von sozialen Medien und Messenger-Diensten sowie um deinen Wissensstand zum Thema Datenschutz in diesem Bezug. Antworte bitte spontan auf die Fragen - es gibt kein Richtig oder Falsch.

Hinweis: Die von dir angegebenen Daten und Antworten lassen keine Rückschlüsse auf deine Person zu. Die Verarbeitung erfolgt ausschließlich zum Zweck dieses Forschungsprojekts.

Personen-Kennung: ID4

Alter: 21

Geschlecht: weiblich
 männlich

1. Nutzt du soziale Medien und/oder Messenger-Dienste?

privat: JA NEIN
beruflich: JA NEIN

2. Welche sozialen Medien und Messenger-Dienste nutzt du?

privat: WhatsApp, TikTok, Instagram, Snapchat und ab und zu Pinterest. Ach so und Tinder, falls das auch dazugehört.

beruflich:

3. Welche Daten musstest du bei der Anmeldung bei den jeweiligen Plattformen/ Diensten angeben?

Name, Geburtsdatum, Wohnort glaub ich, E-Mailadresse, Telefonnummer und dann halt das, was ich noch angeben will. Profil-Foto, Hobbies und so.

4. Hast du dir die Datenschutzrichtlinie der jeweiligen Plattform / des jeweiligen Dienstes durchgelesen?

JA
 NEIN

5. Wenn JA / NEIN, warum?

Nein, das ist mir zu mühsam - verstehe ich sowieso nicht.

6. Was glaubst du, welche Daten die jeweiligen Unternehmen von dir sammeln?

Ja sicher alles mögliche. Alles, was ich dort halt so teile und mache.

7. Siehst du darin irgendwelche Gefahren oder Risiken für dich?

Nein, ich teile ja nichts, das mir irgendwie schaden könnte. Außerdem schauen sich das eh hauptsächlich meine Freunde an und die wissen eh, wie ich bin.

8. Gibt es Informationen, die du lieber nicht mit diesen Unternehmen teilen möchtest?

Ich glaube nicht wirklich. So Krankenstände und Gesundheitssachen würde ich jetzt nicht teilen. Auch nichts, was richtig intim ist. Aber sonst fällt mir nichts ein.

9. Wäre ein Leben ohne soziale Medien und Messenger-Dienste für dich vorstellbar?

JA

NEIN

10. Wenn JA / NEIN, warum?

Mir macht das einfach Spaß! Ich teile gerne meine Videos auf TikTok und schaue mir auch viel an. Mit meinen Freunden kommuniziere ich fast nur dort, das machen irgendwie alle so.

Vielen Dank für das Gespräch!

Fragebogen Nutzung sozialer Medien

Einführung/Erklärung: In dieser Befragung geht es um dein Nutzungsverhalten von sozialen Medien und Messenger-Diensten sowie um deinen Wissensstand zum Thema Datenschutz in diesem Bezug. Antworte bitte spontan auf die Fragen - es gibt kein Richtig oder Falsch.

Hinweis: Die von dir angegebenen Daten und Antworten lassen keine Rückschlüsse auf deine Person zu. Die Verarbeitung erfolgt ausschließlich zum Zweck dieses Forschungsprojekts.

Personen-Kennung: ID5

Alter: 35

Geschlecht: weiblich
 männlich

1. Nutzt du soziale Medien und/oder Messenger-Dienste?

privat: JA NEIN
beruflich: JA NEIN

2. Welche sozialen Medien und Messenger-Dienste nutzt du?

privat: Facebook, Instagram und WhatsApp. Facebook eigentlich nur, um zu sehen, was Leute, die ich kenne, so machen. Tinder hab ich mal genutzt, jetzt aber nicht mehr, seit ich dort meinen Partner kennengelernt hab.

beruflich:

3. Welche Daten musstest du bei der Anmeldung bei den jeweiligen Plattformen/ Diensten angeben?

Das weiß ich gar nicht mehr genau, aber ich schätze mal meinen Namen und die E-Mail-Adresse. Wohnort und Alter wahrscheinlich auch.

4. Hast du dir die Datenschutzrichtlinie der jeweiligen Plattform / des jeweiligen Dienstes durchgelesen?

JA
 NEIN

5. Wenn JA / NEIN, warum?

Da steht ja eh lauter juristisches Zeug drin und das ist mir zu mühsam.

6. Was glaubst du, welche Daten die jeweiligen Unternehmen von dir sammeln?

Ja also die Daten, die ich schon erwähnt habe. Vielleicht auch die Bilder, die ich poste oder die Kommentare die ich schreibe.

7. Siehst du darin irgendwelche Gefahren oder Risiken für dich?

Ich passe generell auf, was ich poste. Ich würde zum Beispiel nie Bilder meines Kindes posten.

8. Gibt es Informationen, die du lieber nicht mit diesen Unternehmen teilen möchtest?

Sicher, alles was mit dem Gesundheitswesen zu tun hat - also von mir oder meiner Familie und mein Gehalt. Das mit dem Datenschutz ist dort sowieso schon so eine Sache. Das muss nicht auch noch dort verbreitet werden.

9. Wäre ein Leben ohne soziale Medien und Messenger-Dienste für dich vorstellbar?

JA

NEIN

10. Wenn JA / NEIN, warum?

Ich denke schon, weil ich eh nicht viel dort poste. Ich sehe mir lieber die Sachen von anderen an. WhatsApp wäre vielleicht etwas schwieriger, weil ich dort mit meiner Familie und Freunden schreibe.

Vielen Dank für das Gespräch!

Fragebogen Nutzung sozialer Medien

Einführung/Erklärung: In dieser Befragung geht es um dein Nutzungsverhalten von sozialen Medien und Messenger-Diensten sowie um deinen Wissensstand zum Thema Datenschutz in diesem Bezug. Antworte bitte spontan auf die Fragen - es gibt kein Richtig oder Falsch.

Hinweis: Die von dir angegebenen Daten und Antworten lassen keine Rückschlüsse auf deine Person zu. Die Verarbeitung erfolgt ausschließlich zum Zweck dieses Forschungsprojekts.

Personen-Kennung: ID6

Alter: 73

Geschlecht: weiblich
 männlich

1. Nutzt du soziale Medien und/oder Messenger-Dienste?

privat: JA NEIN
beruflich: JA NEIN

2. Welche sozialen Medien und Messenger-Dienste nutzt du?

privat: Facebook und WhatsApp

beruflich:

3. Welche Daten musstest du bei der Anmeldung bei den jeweiligen Plattformen/ Diensten angeben?

Die E-Mailadresse und meinen Namen. Alter könnte auch sein und vielleicht meine Adresse.

4. Hast du dir die Datenschutzrichtlinie der jeweiligen Plattform / des jeweiligen Dienstes durchgelesen?

JA
 NEIN

5. Wenn JA / NEIN, warum?

Ich habe mir da eigentlich noch nie Gedanken darüber gemacht, was da drinsteht.

6. Was glaubst du, welche Daten die jeweiligen Unternehmen von dir sammeln?

Keine Ahnung, also wahrscheinlich meine Anschrift und sicher die E-Mailadresse, da kriegt man ja laufend irgendwelche Spam-Mails.

7. Siehst du darin irgendwelche Gefahren oder Risiken für dich?

Ich wüsste nicht welche, ich mache ja nichts, was für die interessant sein könnte.

8. Gibt es Informationen, die du lieber nicht mit diesen Unternehmen teilen möchtest?

Eigentlich nicht, bei mir finden sie eh nicht viel.

9. Wäre ein Leben ohne soziale Medien und Messenger-Dienste für dich vorstellbar?

JA

NEIN

10. Wenn JA / NEIN, warum?

Ja schon. Aber so ist es halt leichter, mit meinem Enkel im Kontakt zu bleiben. Der telefoniert nicht so gerne. Aber schreiben geht immer.

Vielen Dank für das Gespräch!

Fragebogen Nutzung sozialer Medien

Einführung/Erklärung: In dieser Befragung geht es um dein Nutzungsverhalten von sozialen Medien und Messenger-Diensten sowie um deinen Wissensstand zum Thema Datenschutz in diesem Bezug. Antworte bitte spontan auf die Fragen - es gibt kein Richtig oder Falsch.

Hinweis: Die von dir angegebenen Daten und Antworten lassen keine Rückschlüsse auf deine Person zu. Die Verarbeitung erfolgt ausschließlich zum Zweck dieses Forschungsprojekts.

Personen-Kennung: ID7

Alter:

Geschlecht: weiblich
 männlich

1. Nutzt du soziale Medien und/oder Messenger-Dienste?

privat: JA NEIN
beruflich: JA NEIN

2. Welche sozialen Medien und Messenger-Dienste nutzt du?

privat: TikTok, WhatsApp, Snapchat - sonst fällt mir jetzt nix ein. Instagram hab ich auch, aber nutze es kaum.

beruflich:

3. Welche Daten musstest du bei der Anmeldung bei den jeweiligen Plattformen/ Diensten angeben?

Meinen Namen, eine E-Mailadresse und ein Passwort. Alter glaub ich auch zum Teil.

4. Hast du dir die Datenschutzrichtlinie der jeweiligen Plattform / des jeweiligen Dienstes durchgelesen?

JA
 NEIN

5. Wenn JA / NEIN, warum?

Die sind ja immer voll lang. Verstehe eh nicht, was die da so alles schreiben.

6. Was glaubst du, welche Daten die jeweiligen Unternehmen von dir sammeln?

Weiß ich nicht. Sicher die, mit denen sie Geld verdienen können.

7. Siehst du darin irgendwelche Gefahren oder Risiken für dich?

Ich glaub nicht. Hab ich mir eigentlich noch nie so überlegt.

8. Gibt es Informationen, die du lieber nicht mit diesen Unternehmen teilen möchtest?

Ja was ich halt so mit meinen Freunden oder meiner Freundin schreibe. Oder was ich auf dem Konto hab.

9. Wäre ein Leben ohne soziale Medien und Messenger-Dienste für dich vorstellbar?

JA

NEIN

10. Wenn JA / NEIN, warum?

Das geht ja gar nicht. Ich schreib eigentlich nur Sachen übers Handy, telefonieren mag ich nicht. Ohne das würde ich ja keinen erreichen.

Vielen Dank für das Gespräch!

Fragebogen Nutzung sozialer Medien

Einführung/Erklärung: In dieser Befragung geht es um dein Nutzungsverhalten von sozialen Medien und Messenger-Diensten sowie um deinen Wissensstand zum Thema Datenschutz in diesem Bezug. Antworte bitte spontan auf die Fragen - es gibt kein Richtig oder Falsch.

Hinweis: Die von dir angegebenen Daten und Antworten lassen keine Rückschlüsse auf deine Person zu. Die Verarbeitung erfolgt ausschließlich zum Zweck dieses Forschungsprojekts.

Personen-Kennung: ID8

Alter: 41

Geschlecht: weiblich
 männlich

1. Nutzt du soziale Medien und/oder Messenger-Dienste?

privat: JA NEIN
beruflich: JA NEIN

2. Welche sozialen Medien und Messenger-Dienste nutzt du?

privat: Signal, Twitter, WhatsApp und manchal auch YouTube, falls das dazugehört. Skype und Zoom auch manchmal.

beruflich: MS Teams, weil es nicht anders geht und ab und zu auch Zoom.

3. Welche Daten musstest du bei der Anmeldung bei den jeweiligen Plattformen/ Diensten angeben?

Also persönliche Daten wie Name und E-Mailadresse, eventuell auch die Telefonnummer und Kennwort

4. Hast du dir die Datenschutzrichtlinie der jeweiligen Plattform / des jeweiligen Dienstes durchgelesen?

JA
 NEIN

5. Wenn JA / NEIN, warum?

Also nicht generell. Ich hab mir, soweit ich mich noch erinnere, einmal die Mühe gemacht. Aber das ist ja sowieso ein Wahnsinn, was da alles drinsteht.

6. Was glaubst du, welche Daten die jeweiligen Unternehmen von dir sammeln?

Sicher alles, was sie irgendwie kriegen können. Aber ich bin ja nicht wirklich aktiv, sondern schaue mir nur die Sachen von anderen an. Auch auf Instagram oder Twitter, dafür muss ich mich nicht unbedingt anmelden.

7. Siehst du darin irgendwelche Gefahren oder Risiken für dich?

Ich denke, so lange ich nicht irgendwie gehackt werde und irgendwer private Sachen dort verbreitet ist das Risiko nicht besonders groß. Im beruflichen Umfeld wären es vielleicht Messdaten, aber mit denen kann auch nicht jeder was anfangen.

8. Gibt es Informationen, die du lieber nicht mit diesen Unternehmen teilen möchtest?

Klar! Alles was meine Gesundheit betrifft oder genetische Daten, Fingerabdrücke usw. Und meine Gehaltszettel würde ich auch nicht gerne mit denen teilen.

9. Wäre ein Leben ohne soziale Medien und Messenger-Dienste für dich vorstellbar?

- JA
 NEIN

10. Wenn JA / NEIN, warum?

Eigentlich schon, aber es ist halt schon sehr praktisch, wenn man beispielsweise in Gruppen kommunizieren kann. Also auf soziale Medien eher als auf die Messenger-Dienste.

Vielen Dank für das Gespräch!

Fragebogen Nutzung sozialer Medien

Einführung/Erklärung: In dieser Befragung geht es um dein Nutzungsverhalten von sozialen Medien und Messenger-Diensten sowie um deinen Wissensstand zum Thema Datenschutz in diesem Bezug. Antworte bitte spontan auf die Fragen - es gibt kein Richtig oder Falsch.

Hinweis: Die von dir angegebenen Daten und Antworten lassen keine Rückschlüsse auf deine Person zu. Die Verarbeitung erfolgt ausschließlich zum Zweck dieses Forschungsprojekts.

Personen-Kennung: ID9

Alter: 33

Geschlecht: weiblich
 männlich

1. Nutzt du soziale Medien und/oder Messenger-Dienste?

privat: JA NEIN
beruflich: JA NEIN

2. Welche sozialen Medien und Messenger-Dienste nutzt du?

privat: Instagram, Facebook, Pinterest, WhatsApp und Tinder

beruflich:

3. Welche Daten musstest du bei der Anmeldung bei den jeweiligen Plattformen/ Diensten angeben?

Den Namen, einen Profilnamen, Kennwort, E-Mail-Adresse, Wohnort und Alter. Und sonst die Interessen, Geschlecht und so Sachen. Das ist aber freiwillig glaub ich.

4. Hast du dir die Datenschutzrichtlinie der jeweiligen Plattform / des jeweiligen Dienstes durchgelesen?

JA
 NEIN

5. Wenn JA / NEIN, warum?

Da hab ich mir eigentlich noch nie Gedanken gemacht. Meistens scrolle ich da drüber und klicke dann auf ‚OK‘. Sonst kann man ja eh nichts damit machen.

6. Was glaubst du, welche Daten die jeweiligen Unternehmen von dir sammeln?

Ich denke mal alles, was ich dort so poste oder reingeschrieben habe.

7. Siehst du darin irgendwelche Gefahren oder Risiken für dich?

Nicht wirklich. Auf Instagram poste ich meine Fotografien, die ich so anfertige. Sonst meistens Bilder von Reisen oder neuen größeren Sachen, die ich gekauft habe.

8. Gibt es Informationen, die du lieber nicht mit diesen Unternehmen teilen möchtest?

Auf jeden Fall alles, was meine Gesundheit betrifft, Krankenakten, Krankenstände, Medikamente usw. Naja und Details über mein Intimleben, die gehen auch niemanden etwas an.

9. Wäre ein Leben ohne soziale Medien und Messenger-Dienste für dich vorstellbar?

- JA
 NEIN

10. Wenn JA / NEIN, warum?

Ich nutze diese Plattformen gerne, weil ich mich über mein Hobby mit anderen austauschen kann und auch sehe, was die so machen. Und mit WhatsApp kann ich auch viel schneller jemanden aus meiner Familie oder meine Freunde erreichen. Ich bin generell nicht jemand, der gerne telefoniert.

Vielen Dank für das Gespräch!

Fragebogen Nutzung sozialer Medien

Einführung/Erklärung: In dieser Befragung geht es um dein Nutzungsverhalten von sozialen Medien und Messenger-Diensten sowie um deinen Wissensstand zum Thema Datenschutz in diesem Bezug. Antworte bitte spontan auf die Fragen - es gibt kein Richtig oder Falsch.

Hinweis: Die von dir angegebenen Daten und Antworten lassen keine Rückschlüsse auf deine Person zu. Die Verarbeitung erfolgt ausschließlich zum Zweck dieses Forschungsprojekts.

Personen-Kennung: ID10

Alter: 28

Geschlecht: weiblich
 männlich

1. Nutzt du soziale Medien und/oder Messenger-Dienste?

privat: JA NEIN
beruflich: JA NEIN

2. Welche sozialen Medien und Messenger-Dienste nutzt du?

privat: WhatsApp, TikTok, Snapchat, Instagram. Bei Meta habe ich mich auch angemeldet.

beruflich: WhatsApp, vor allem, wenn ich auf Baustellen unterwegs bin.

3. Welche Daten musstest du bei der Anmeldung bei den jeweiligen Plattformen/ Diensten angeben?

Name, Geburtsdatum, E-Mail-Adresse. Geschlecht könnte auch noch sein. Dann halt meistens den Profil-Namen und ein Bild.

4. Hast du dir die Datenschutzrichtlinie der jeweiligen Plattform / des jeweiligen Dienstes durchgelesen?

JA
 NEIN

5. Wenn JA / NEIN, warum?

Nein, die sind ja meistens ewig lang. Ich weiß auch nicht, ob ich das alles verstehen würde.

6. Was glaubst du, welche Daten die jeweiligen Unternehmen von dir sammeln?

Ja also meine ganzen Anmeldedaten und das was ich so poste, sonst könnte man wahrscheinlich auch keinen Account mehr herstellen. Mehr fällt mir nicht ein.

7. Siehst du darin irgendwelche Gefahren oder Risiken für dich?

Eigentlich nicht, also zumindest so lange ich nicht selbst einen Blödsinn dort verbreite. Aber das mache ich ja nicht.

8. Gibt es Informationen, die du lieber nicht mit diesen Unternehmen teilen möchtest?

Alles, was mit finanziellen Dingen zu tun hat. Also Kredite zum Beispiel, Gehalt, was ich so einkaufe. Die Daten vom Arzt wären sicher auch nicht ideal.

9. Wäre ein Leben ohne soziale Medien und Messenger-Dienste für dich vorstellbar?

- JA
- NEIN

10. Wenn JA / NEIN, warum?

Es ist einfach praktisch. Dort ist irgendwie jeder immer irgendwie erreichbar. Das spart Zeit, weil ich auch mehreren Leuten gleichzeitig schreiben kann. Ich würde es jedenfalls seltsam finden, wenn das nicht mehr so wäre.

Vielen Dank für das Gespräch!

Datenrichtlinie Meta

Was ist die Datenrichtlinie und was behandelt sie? Gültig ab 26. Juli 2022. Wir bei Meta möchten, dass du verstehst, welche Informationen wir erheben und wie wir sie verwenden und teilen. Deshalb empfehlen wir dir, unsere Datenrichtlinie zu lesen. Auf diese Weise kannst du die Meta-Produkte ganz nach deinen Wünschen nutzen. In der Datenrichtlinie erläutern wir, wie wir Informationen erheben, verwenden, teilen, speichern und übermitteln. Wir informieren dich außerdem über deine Rechte. Jeder Abschnitt der Richtlinie enthält hilfreiche Beispiele und eine vereinfachte Sprache, um unsere Praktiken leichter verständlich zu machen. Außerdem haben wir Links zu den Ressourcen hinzugefügt, über die du mehr zu den Datenschutzthemen erfahren kannst, die dich interessieren. Es ist uns wichtig, dass du weißt, wie du deine Privatsphäre kontrollierst. Deshalb zeigen wir dir auch, wo du deine Informationen in den Einstellungen der von dir genutzten Meta-Produkte verwalten kannst. Du kannst diese Einstellungen aktualisieren, um dein Nutzungserlebnis anzupassen. Die vollständige Richtlinie findest du nachstehend. Welche Produkte behandelt diese Richtlinie? Diese Richtlinie beschreibt die Informationen, die wir, Meta Platforms Ireland Limited, verarbeiten, um Meta-Produkte bereitzustellen. Meta-Produkte, auch „Produkte“ genannt, umfassen: Facebook, Messenger, Instagram (einschließlich Apps wie Boomerang), Facebook Portal-Produkte, Produkte von Meta Platforms Technologies (wenn sie mit einem Facebook-Konto verknüpft sind), Shops, Marketplace, Spark AR, Meta-Business-Tools, Meta Audience Network, NPE Team-Apps, Facebook View. Einige unserer Produkte haben auch ergänzende Datenrichtlinien, die die in dieser Richtlinie bereitgestellten Informationen erweitern. Welche Informationen erheben wir? Die Arten der von uns über dich erhobenen Informationen hängen davon ab, wie du unsere Produkte nutzt. Zum Beispiel erheben wir andere Informationen, wenn du Möbel im Marketplace verkaufst, als wenn du ein Reel auf Instagram postest. Wenn du unsere Produkte nutzt, erheben wir einige Informationen über dich, auch wenn du kein Konto hast. Diese Informationen erheben wir: Deine Aktivität und die von dir bereitgestellten Informationen: Auf unseren Produkten kannst du Nachrichten senden, Fotos und Videos aufnehmen, Dinge kaufen oder verkaufen und vieles mehr. Wir nennen all die Dinge, die du auf unseren Produkten tun kannst, „Aktivität“. Wir erfassen deine Aktivität auf allen unseren Produkten sowie die Informationen, die du uns bereitstellst, wie z. B.: Inhalte, die du erstellst, wie Beiträge oder Kommentare oder Audio; Inhalte, die du über unsere Kamerafunktion oder deine Einstellungen für Aufnahmen oder über unsere sprachgestützten Funktionen bereitstellst. Mehr dazu, welche Informationen wir von diesen Funktionen erfassen, und wie wir Informationen von der Kamera für Masken, Filter, Avatare und Effekte verwenden. Nachrichten, die du sendest und empfangst, einschließlich ihrer Inhalte, vorbehaltlich des geltenden Rechts. Wir können jedoch nicht die Inhalte von Ende-zu-Ende-verschlüsselten Nachrichten einsehen, es sei denn, sie werden uns zur Überprüfung gemeldet. Metadaten zu Inhalten und Nachrichten, vorbehaltlich des geltenden Rechts; Die Arten von Inhalten, die du dir ansiehst bzw. mit denen du interagierst, Die Apps und Funktionen, die du nutzt, und welche Handlungen du in ihnen durchführst. Einige Beispiele. Käufe, die du tätigt, oder andere Transaktionen, die du durchführst, einschließlich Kreditkartendaten. Hashtags, die du verwendest. Den Zeitpunkt, die Häufigkeit und die Dauer deiner Aktivitäten auf unseren Produkten Aufrufe einer Facebook-Seite und ihrer Inhalte sowie Interaktionen mit dieser bzw. diesen, um dem Seitenadministrator aggregierte Informationen dazu bereitzustellen, wie Personen seine Seite und deren Inhalte nutzen. Meta ist gemeinsam mit den Seitenadministratoren verantwortlich. Mehr zur gemeinsamen Verarbeitung für Seiten-Insights. Informationen mit besonderem Schutz Du kannst in deinen Facebook-Profilfeldern Informationen über deine religiösen Ansichten, deine politischen Einstellungen oder an wem du „interessiert“ bist angeben (was deine sexuelle Orientierung verraten könnte). Diese und andere Informationen (wie rassische oder ethnische Herkunft, weltanschauliche Überzeugungen oder Gewerkschaftszugehörigkeit) unterliegen nach dem Recht deines Landes einem besonderen Schutz. Freunde, Follower und andere Kontakte Informationen, die wir über deine Freunde, Abonnenten und anderen Kontakte erfassen Wir erfassen Informationen über Freunde, Abonnenten, Gruppen, Konten, Facebook-Seiten und andere Nutzer und Gemeinschaften, mit denen du vernetzt bist und mit denen du interagierst. Dazu gehört, wie du mit ihnen in unseren Produkten interagierst, und mit welchen du am meisten interagierst. Informationen, die wir über Kontakte erheben: Wir erheben auch Informationen deiner Kontakte, wie z. B. ihren Namen und ihre E-Mail-Adresse oder ihre Telefonnummer, wenn du diese von einem Gerät hochlädst oder importierst, wie durch das Synchronisieren eines Adressbuchs. Wenn du keine Meta-Produkte nutzt oder sie ohne Konto nutzt, könnten deine Informationen dennoch erhoben werden. Erfahre mehr dazu, wie Meta Kontaktinformationen verwendet, die von Kontoinhabern hochgeladen werden. Erfahre, wie du Kontakte auf Facebook und in den bzw. im Messenger hochlädst bzw. löschst, und wie du auf Instagram die Kontaktliste deines Geräts verknüpfst. Informationen, die wir basierend auf der Aktivität anderer über dich erfassen bzw. ableiten

Basierend auf der Aktivität anderer erheben wir Informationen über dich. Einige Beispiele: Basierend auf der Aktivität anderer leiten wir auch Informationen über dich ab. Zum Beispiel: Wir können dir über die Facebook-Funktion „Personen, die du kennen könntest“ eine/n Freund/in vorschlagen, wenn ihr beide in einer Kontaktliste aufgeführt seid, die jemand hochlädt. Wir berücksichtigen, ob deine Freunde einer Gruppe angehören, wenn wir dir vorschlagen, ihr beizutreten. App-, Browser- und Geräteinformationen; Wir erfassen und erhalten Informationen von den bzw. über die verschiedenen von dir genutzten Geräte(n) – auch wie du sie nutzt. Geräteinformationen, die wir erheben und erhalten, umfassen u. a.: Das/die von dir genutzte Gerät bzw. Software sowie andere Geräteeigenschaften. Einige Beispiele. Was du gerade auf deinem Gerät tust, z. B. ob sich unsere App im Vordergrund befindet oder ob sich deine Maus bewegt (dadurch lassen sich Menschen von Robotern unterscheiden). Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, wie u. a. Family Device IDs. Einige Beispiele. Signale von deinem Gerät. Einige Beispiele. Informationen, die du mit uns über die Geräteeinstellungen geteilt hast, wie GPS-Standort, Kamerazugriff, Fotos und zugehörige Metadaten, Informationen zum Netzwerk, mit dem du dein Gerät verbindest, einschließlich deiner IP-Adresse. Weitere Beispiele. Informationen über die Performance unserer Produkte auf deinem Gerät. Informationen von Cookies und ähnlichen Technologien. Mehr dazu. Informationen von Partnern, Anbietern und Dritten. Welche Arten von Informationen erheben bzw. erhalten wir? Wir erheben und erhalten Informationen von Partnern, Anbietern für Messlösungen und Dritten zu vielen deiner Informationen und Aktivitäten auf und außerhalb von unseren Produkten. Hier sind einige Beispiele für Informationen, die wir über dich erhalten: Deine Geräteinformationen, Websites, die du besuchst, und Cookie-Daten, etwa durch soziale Plugins oder das Meta-Pixel; Apps, die du nutzt; Spiele, die du spielst; Käufe, die du tätigt, und Transaktionen, die du durchführst; Werbeanzeigen, die du dir ansiehst, und wie du mit ihnen interagierst; Wie du die Produkte und Dienste bzw. Dienstleistungen unserer Partner online oder persönlich nutzt. Partner teilen auch Informationen wie deine E-Mail-Adresse, Cookies und deine Geräte-ID für Werbezwecke mit uns. Diese Informationen helfen uns dabei, deine Aktivitäten mit deinem Konto abzugleichen, wenn du eines hast. Wir erhalten diese Informationen unabhängig davon, ob du bei unseren Produkten angemeldet bist bzw. ein Konto auf ihnen hast oder nicht. Mehr dazu, wie wir Informationen von Partnern mit deinem Konto verknüpfen. Partner geben außerdem ihre Kommunikation mit dir an uns weiter, wenn sie uns anweisen, Dienstleistungen für ihr Unternehmen zu erbringen, wie Unterstützung bei der Verwaltung ihrer Kommunikation. Um zu erfahren, wie ein Unternehmen deine Informationen verarbeitet und teilt, lies dessen Datenschutzrichtlinie oder kontaktiere es direkt. Übernimm die Kontrolle: Aktivitäten außerhalb von Facebook; Cookie-Einstellungen. Wie erheben oder erhalten wir diese Informationen von Partnern? Partner nutzen unsere Business-Tools, Integrationen und Meta Audience Network-Technologien, um Informationen mit uns zu teilen. Diese Partner erheben deine Informationen, wenn du ihre Website oder App besuchst oder ihre Dienste nutzt, oder über andere Unternehmen oder Organisationen, mit denen sie zusammenarbeiten. Wir verlangen von Partnern, dass sie das Recht zur Erhebung, zur Verwendung und zum Teilen deiner Informationen haben, bevor sie sie an uns weitergeben. Wir verarbeiten bestimmte Informationen, die wir von Partnern erhalten, als gemeinsam Verantwortlicher mit ihnen. Mehr zu unseren Vereinbarungen mit diesen Partnern. Was ist, wenn du uns die Erhebung bestimmter Informationen nicht gestattest? Einige Informationen sind erforderlich, damit unsere Produkte funktionieren. Andere Informationen sind optional, ohne sie könnte jedoch die Qualität deines Erlebnisses beeinträchtigt werden. Übernimm die Kontrolle im Privacy Center

Verwalte die Informationen, die wir über dich erheben Informationen, die wir erheben, wenn du unsere Produkte nutzt, aber kein Konto hast. Wir erheben beispielsweise folgende Informationen: Browser- und App-Protokolle über deine Besuche von öffentlichen Inhalten, wie Facebook-Seiten, Videos und Räumen; Basisinformationen über Geräte, die unsere Apps heruntergeladen haben, darunter Gerätemodell und Betriebssystem. Wir erhalten außerdem Informationen mithilfe von Cookies und ähnlichen Technologien wie dem Meta-Pixel oder sozialen Plugins, wenn du andere Websites und Apps besuchst, die Meta-Produkte verwenden. Lies dir unsere Cookie-Richtlinie durch, um mehr zu erfahren. Darum erheben wir Informationen: Sicherheit unserer Produkte: Wenn wir beispielsweise bemerken, dass jemand ohne Konto versucht, zu viele Seiten zu laden, könnte diese Person versuchen, unsere Website unter Verstoß gegen unsere Nutzungsbedingungen zu scrapen. In diesem Fall können wir Maßnahmen ergreifen, um dies zu unterbinden. Sicherheit und Integrität: Wenn zum Beispiel jemand ohne Konto einem Raum beitrifft und ein gefährliches Video teilt, können wir gemäß unseren Gemeinschaftsstandards Maßnahmen ergreifen. Wir können Inhalte entfernen, die gegen unsere Nutzungsbedingungen und Richtlinien verstoßen, oder Informationen an Strafverfolgungsbehörden weitergeben, wenn wir der Ansicht sind, dass ernsthafte Lebensgefahr oder das Risiko einer unmittelbar bevorstehenden Körperverletzung besteht. Performance: Wir nutzen zum Beispiel Informationen, die wir über Personen haben, die unsere Produkte nutzen, auch wenn sie kein

Konto haben, um zu messen, wir schnell unsere Seiten in verschiedenen Ländern laden. Dies hilft uns bei der Erkennung und Behebung von Problemen, die in lokalen Netzwerken auftreten. Von dir bereitgestellte Informationen: Wenn du zum Beispiel ein Facebook-Konto erstellst, musst du einige Informationen bereitstellen, darunter ein Passwort und deine E-Mail-Adresse oder Telefonnummer. Es bleibt dir überlassen, ob du in deinem Konto weitere Details angibst, wie beispielsweise ein Profilbild oder Zahlungsinformationen. Wir erheben außerdem Informationen, die du bereitstellst, wenn du: deinen Avatar erstellst; ein Formular ausfüllst; uns kontaktierst. Von dir erstellte Audioinhalte: Du kannst Audioinhalte erstellen, z. B. wenn du einen Live Audio Room hostest oder daran teilnimmst. Jeder im Publikum für die Übertragung kann Live-Audio anhören. Was wir über unsere Kamera-Funktion erheben: José nutzt gerne die Kamera-Funktion von Instagram, um Fotos seiner Freunde und Freundinnen zu machen. Wir erheben Informationen darüber, wie José die Kamera-Funktion nutzt, einschließlich was er durch die Kameralinse seines Geräts sieht, während er die Funktion nutzt. Das hilft uns dabei, Masken und Filter vorzuschlagen, die ihm gefallen könnten. So funktionieren Filter, Effekte, Masken und Avatare: Wenn du unsere Kamera nutzt oder Zugriff auf Fotos und Videos gewährest, kannst du bei bestimmten Meta-Produkten Filter, Effekte, Masken oder Avatare hinzufügen. Einige dieser Funktionen verarbeiten Teile von Gesichtern oder Körpern im Bild der Kamera, Foto oder Video. Dadurch können sie beispielsweise eine Maske richtig über Augen, Nase und Mund platzieren. Die von uns hierfür verwendeten Informationen werden für die Erstellung der Funktion genutzt. Sie werden nicht verwendet, um dich zu identifizieren. Was wir über sprachunterstützte Funktionen erheben: Ren sagt dem sprachunterstützten Assistant von Meta, er soll ein Foto der Ray-Ban Stories aufnehmen. Ein visueller Indikator gibt an, dass der Assistant aktiviert ist und auf Rens gesprochene Befehle wartet. Wir erfassen diese Sprachinteraktion, die jegliche Hintergrundgeräusche enthält, die bei Rens Befehl zu hören sind. Das Erheben von Rens Sprachinteraktionen ermöglicht uns die Bereitstellung und – je nach Rens Einstellungen – Verbesserung der Assistant-Funktion. Metadaten zu Inhalten oder Nachrichten: Metadaten sind: Informationen über die Inhalte, wie zum Beispiel der Ort, an dem das Foto aufgenommen wurde, oder das Erstellungsdatum einer Datei; Informationen über die Nachricht, wie zum Beispiel die Art der Nachricht oder Datum und Uhrzeit, wann sie gesendet wurde; Apps und Funktionen, die du nutzt, und wie du sie nutzt. Wir protokollieren beispielsweise folgende Informationen: Welche Apps, Posts, Videos, Werbeanzeigen, Spiele, Shops und andere Inhalte du über unsere Produkte anzeigst oder verwendest; Wenn du soziale Plugins, Facebook Login oder automatisches Ausfüllen nutzt; Käufe oder andere Transaktionen. Wir erheben Informationen, wenn du unsere Produkte nutzt, um Dinge zu kaufen oder zu verkaufen oder andere finanzielle Transaktionen zu tätigen. Einige Beispiele: Käufe in einem Online-Spiel; Spenden an die Spendenaktion eines Freundes/einer Freundin; Käufe im Marketplace, in Shops oder Gruppen; Geldtransfers an Freunde und Familie (sofern verfügbar). Was wir von Transaktionen erheben. Wenn du Käufe oder andere Zahlungen im Marketplace, in Shops oder Gruppen tätigest, erheben wir Informationen über deinen Kauf oder deine anderen finanziellen Transaktionen, wie z.B.: Kredit- oder Debitkartennummer und andere Karteninformationen; Rechnungs-, Versand- und Kontaktinformationen; gekaufte Artikel und deren Anzahl; andere Konto- und Authentifizierungsinformationen. Darum erheben wir diese Informationen: Wir speichern diese Informationen unter anderem, um dir den Zugriff auf und die Einsicht in deinen Zahlungs- und Transaktionsverlauf zu ermöglichen. Außerdem kannst du dadurch deine nächste Shoppingerfahrung einfacher und schneller gestalten. Wann wir Informationen basierend auf der Aktivität anderer erheben. Zum Beispiel erheben wir Informationen über dich auf Meta-Produkten, wenn andere: ein Foto teilen oder kommentieren, auf dem du markiert bist; dir eine Nachricht schicken; dich zu einer Unterhaltung einladen; ihr Adressbuch hochladen, das deine Kontaktinformationen enthält; dich zu einem Spiel einladen. Geräte: Darunter fallen Computer, Telefone, Hardware, Connected TVs, Portal-Geräte und andere mit dem Netz verbundene Geräte. Das von dir genutzte Gerät sowie andere Geräteeigenschaften: Diese Geräteinformationen erheben wir u. a.: die Art des Geräts; Informationen zum Betriebssystem; Informationen zur Hardware und Software; Akkuladestatus; Signalstärke; verfügbarer Speicher; Browserart; App- und Dateinamen und -typen; Plug-ins. Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden. Zu den Kennungen, die wir erheben, gehören Geräte-IDs, Mobile Advertiser IDs oder IDs von Spielen, Apps oder Konten, die du nutzt. Wir erheben auch Family Device IDs oder sonstige Kennungen, die für die mit demselben Gerät oder Konto verknüpften Produkte der Meta-Unternehmen eindeutig sind. Gerätesignale; Gerätesignale umfassen GPS, Bluetooth-Signale, Wi-Fi-Zugriffspunkte, Beacons und Mobilfunkmasten in der Nähe. Zugehörige Metadaten: Wenn du uns zum Beispiel Zugriff auf die Kameraaufnahmen deines Geräts gewährest, erheben wir Metadaten. Diese Metadaten stammen von deinen Fotos und Videos und enthalten Datum und Uhrzeit der Aufnahme. Wir nutzen diese Informationen beispielsweise, um dich daran zu erinnern, wenn du neue Fotos zum Hochladen hast. Informationen zum Netzwerk, mit dem du dein Gerät verbindest: Informationen zu deinem Netzwerk umfassen: den Namen deines Mobilfunkanbieters oder Internetanbieters, Sprache, Zeitzone, Mobilfunknummer, IP-Adresse,

Verbindungsgeschwindigkeit, Informationen zu anderen Geräten in der Nähe oder in deinem Netzwerk, WLAN-Hotspots, mit denen du dich über unsere Produkte verbindest. Wir erheben diese Informationen unter anderem, um deine Erfahrung zu verbessern. Wenn wir zum Beispiel wissen, dass dein Telefon und Fernseher mit demselben Netzwerk verbunden sind, können wir dir dabei helfen, dein Telefon zu verwenden, um einen Video-Stream auf deinem Fernseher zu steuern.

Informationen über die Performance unserer Produkte auf deinem Gerät: Wir erheben Geräteinformationen, um Fehler zu vermeiden, zu analysieren, zu erkennen und zu beheben. Unter diese Informationen fallen die Laufzeit einer App, das Gerätemodell und andere Leistungs- und diagnostische Informationen. Cookies: Cookies sind kleine Textstücke, die zum Speichern von Informationen in Webbrowsern verwendet werden. Wir nutzen Cookies und ähnliche Technologien, einschließlich der von uns in deinem Webbrowser oder Gerät gespeicherten Daten, der mit deinem Gerät verknüpften Kennungen sowie sonstiger Software, soziale Plugins und das Meta-Pixel. Sie helfen uns dabei, unsere Produkte bereitzustellen, sie zu schützen und zu verbessern; beispielsweise indem wir Inhalte personalisieren, Werbeanzeigen individuell anpassen und messen bzw. ein sichereres Erlebnis bieten. Wir erheben Informationen von auf deinem Gerät gespeicherten Cookies, einschließlich Cookie-IDs und -Einstellungen. Unsere Cookie-Richtlinien lesen: Cookie-Richtlinie von Facebook: Cookie-Richtlinie von Instagram. Unsere Partner: Unternehmen und Personen können unsere Produkte nutzen, um ihre Produkte und Dienste zu bewerben, zu vertreiben oder zu unterstützen. Wenn sie unsere Produkte nutzen, nennen wir sie unsere Partner. Zu unseren Produkten gehören Business-Tools und andere Technologien, mit denen Unternehmen ihre Produkte und Dienstleistungen bewerben oder unterstützen oder feststellen und messen können, wie ihre Dienstleistungen genutzt werden und wie gut ihre Anzeigen funktionieren. Beispielsweise können sie eines unserer Business-Tools, das Meta-Pixel, auf ihrer Website platzieren. Oder sie verwenden die Meta Audience Network-Tools, um mit ihren Apps Geld zu verdienen, indem sie Werbeanzeigen von Unternehmen zeigen, die Werbung auf Facebook schalten. Zu unseren Produkten gehören außerdem Technologien, mit denen über unsere Produkte eine Verbindung zu unseren Partnern hergestellt werden kann. Denkbar ist beispielsweise, dass du dich über Facebook Login bei deren App oder Website anmeldest. Oder du spielst deren Spiel auf Facebook. Das nennen wir eine Integration, denn du kannst spielen, ohne unsere App zu verlassen. Wir nennen die Partner, die diese integrierten Tools nutzen, unsere integrierten Partner. Hier sind ein paar Beispiele: Werbetreibende, Unternehmen, die die Effektivität der Werbeanzeigen messen und Berichte erstellen, Unternehmen und Personen, die unsere Produkte verwenden, um Waren und Dienstleistungen zu verkaufen oder anzubieten. Publisher (wie eine Website oder App) und deren Geschäftspartner, App-Entwickler, Spieleentwickler, Dritte, von denen wir Informationen erhalten: Andere Organisationen und Stellen geben Informationen an Meta weiter, nutzen unsere Produkte jedoch nicht. Wir bezeichnen sie als Dritte oder Drittanbieter. Wir erheben und erhalten Informationen von diesen Dritten, darunter: öffentlich zugängliche Quellen, wie akademische Aufsätze und öffentliche Foren, Branchenkollegen, wie zum Beispiel andere Online-Plattformen und Technologieunternehmen, Marketing- und Werbungsanbieter sowie Datenanbieter, die das Recht haben, uns deine Informationen zur Verfügung zu stellen, Strafverfolgungsbehörden, Regierungsbehörden, Berufsgruppen und gemeinnützige Gruppen wie NGOs und Wohltätigkeitsorganisationen, akademische und Forschungsinstitutionen, z. B. Universitäten, gemeinnützige Forschungsorganisationen und Denkfabriken. Öffentliche Quellen Dritter: Zum Beispiel erhalten wir Datensätze von öffentlich zugänglichen Quellen, Forschungsinstitutionen, Berufsgruppen und gemeinnützigen Organisationen. Wir nutzen diese Datensätze für folgende Zwecke: Erkennen und Stoppen von gegen unsere Nutzungsbedingungen verstoßendem Scraping, Ergreifen von Maßnahmen zur Förderung von Schutz, Integrität und Sicherheit für unsere Produkte, Nutzer, die Öffentlichkeit sowie unsere Mitarbeiter und unser Eigentum, Verbessern unserer KI-Technologien, wie z. B. Übersetzungen, Unterstützen von KI-Forschung, wie z. B. Bilderkennungs- und natürliche Sprachverarbeitungstechnologie, Austausch mit Teilnehmer/innen aus Forschungsumfragen, die an weiterführenden Gesprächen interessiert sind. Was ist, wenn du uns die Erhebung bestimmter Informationen nicht gestattest? Wenn du beispielsweise keine E-Mail-Adresse oder Telefonnummer angibst, können wir für dich kein Konto zur Nutzung unserer Produkte erstellen. Oder du kannst entscheiden, keine Facebook-Freunde hinzuzufügen, aber dann zeigt dein Facebook-Feed keine Fotos oder Status-Updates von Freunden. Wie verwenden wir deine Informationen? Wir verwenden Informationen, die wir erheben, um dir personalisierte Erlebnisse, einschließlich Werbeanzeigen, zur Verfügung zu stellen sowie für die anderen Zwecke, die wir unten ausführlich darlegen. Für einige dieser Zwecke verwenden wir Informationen übergreifend über alle unsere Produkte und alle deine Geräte hinweg. Die von uns für diese Zwecke verwendeten Informationen werden automatisch von unseren Systemen verarbeitet. In einigen Fällen nutzen wir jedoch auch eine manuelle Überprüfung, um auf deine Informationen zuzugreifen und sie zu überprüfen. Um weniger Informationen zu verwenden, die mit einzelnen Nutzern verknüpft sind, de-identifizieren wir Informationen in einigen Fällen oder aggregieren diese. Wir können sie auch anonymisieren, sodass es nicht mehr möglich ist,

dich durch sie zu identifizieren. Wir verwenden diese Informationen auf dieselbe Art und Weise, wie wir deine Informationen verwenden – also so, wie es in diesem Abschnitt beschrieben ist. So verwenden wir deine Informationen: Zur Bereitstellung, Personalisierung und Verbesserung unserer Produkte: Wir verwenden die uns zur Verfügung stehenden Informationen, um unsere Produkte bereitzustellen und zu verbessern. Dies umfasst das Personalisieren von Funktionen, Inhalten und Empfehlungen, wie z. B. deinen Facebook-Feed, deinen Instagram-Feed, deine Stories und Werbeanzeigen. Wir verwenden die von dir für diese Zwecke freiwillig bereitgestellten Informationen mit besonderem Schutz, aber nicht, um dir Werbeanzeigen zu zeigen. Weitere Infos dazu, wie wir Informationen verwenden, um unsere Produkte bereitzustellen, zu personalisieren und zu verbessern: So zeigen wir Werbeanzeigen und andere gesponserte bzw. kommerzielle Inhalte. Wenn du unsere Produkte nutzt, siehst du Werbeanzeigen und gesponserte bzw. kommerzielle Inhalte, wie z. B. Produktinserate in Shops. Du siehst auch Werbeanzeigen, die über das Meta Audience Network gezeigt werden, wenn du andere Apps besuchst. Wir möchten, dass alles, was du siehst, interessant und nützlich für dich ist. Um zu entscheiden, was wir dir und anderen zeigen, verwenden wir die Informationen, die wir über dich haben, wie u. a.: **Deine Profilinformationen, Deine Aktivität auf und außerhalb von unseren Produkten, darunter Informationen, die wir durch Cookies und ähnliche Technologien erhalten, gemäß deinen Einstellungen, Dinge, die wir über dich ableiten, wie Themen, von denen wir denken, dass sie dich interessieren könnten, Informationen über deine Freunde, Abonnenten bzw. anderen Kontakte, einschließlich ihrer Aktivitäten oder Interessen.** So verwenden wir Informationen, um unsere Produkte zu verbessern: Wir versuchen stets, unsere Produkte zu verbessern und neue zu entwickeln, mit den Funktionen, die ihr möchtet. Die Informationen, die wir von dir erheben, helfen uns dabei. Wir verwenden die von uns erhobenen Informationen zu folgenden Zwecken: Sehen, ob ein Produkt ordnungsgemäß funktioniert, Nach Fehlern suchen und diese gegebenenfalls beheben, Neue Produkte und Funktionen testen, um deren Funktionalität zu prüfen, Feedback zu unseren Ideen für Produkte oder Funktionen einholen, Durchführung von Umfragen und anderen Studien dazu, was dir an unseren Produkten und Marken gefällt und was wir noch besser machen können. So verwenden wir standortbezogene Informationen: **Wir verwenden standortbasierte Informationen, deren Erhalt du uns gestattest, wenn du die Geräteeinstellung „Ortungsdienste“ aktivierst. Dies umfasst u. a. deinen GPS-Standort und, je nach dem von dir verwendeten Betriebssystem, andere Gerätesignale.** Wir erhalten und verwenden außerdem einige **standortbezogene Informationen, und zwar auch dann, wenn die Ortungsdienste ausgeschaltet sind.** Dazu gehören: **IP-Adressen**, die wir verwenden, um deinen allgemeinen Standort zu schätzen. Wir können IP-Adressen verwenden, um deinen konkreten Standort zu schätzen, wenn dies erforderlich ist, um deine Sicherheit oder die anderer zu schützen. **Deine Aktivität und die anderer auf unseren Produkten, wie Besuche und Veranstaltungen, Informationen, die du uns direkt bereitstellst, beispielsweise wenn du deinen aktuellen Wohnort in deinem Profil angibst oder deine Adresse in Marketplace nennst.** Wir verwenden standortbezogene Informationen – wie deinen aktuellen Standort, deinen Wohnort, die Orte, die du gerne besuchst, und die Unternehmen und Personen in deiner Nähe – um die im Abschnitt „Wie verwenden wir deine Informationen?“ der Richtlinie beschriebenen Dinge zu tun, wie z. B.: Bereitstellung, Personalisierung und Verbesserung unserer Produkte, einschließlich Werbeanzeigen, für dich und andere. Ein Beispiel ansehen. Erkennung verdächtiger Aktivitäten und Unterstützung beim Schutz deines Kontos, um den Schutz, die Integrität und die Sicherheit zu fördern. Wir verwenden die von uns erhobenen Informationen, um unsere Nutzer vor Schaden zu schützen und um sichere Produkte bereitzustellen. Zur Bereitstellung von Messungs- und Analysediensten sowie Unternehmens-Services: Viele Menschen setzen auf unsere Produkte, um ihre Unternehmen zu betreiben bzw. zu bewerben. Wir unterstützen sie dabei, zu messen, wie gut ihre Werbeanzeigen und sonstigen Inhalte funktionieren. Für die Kommunikation mit dir: Wir kommunizieren mit dir unter Verwendung der Informationen, die du uns bereitgestellt hast, wie z. B. Kontaktinformationen, die du in deinem Profil angegeben hast. Für Forschung und Innovation für soziale Zwecke: Wir verwenden uns zur Verfügung stehende Informationen, Informationen von Forschern sowie Datensätze aus öffentlich zugänglichen Quellen, von Berufsgruppen und von gemeinnützigen Organisationen, um Forschung durchzuführen und zu unterstützen. Förderung von Datenschutz, Sicherheit und Integrität: Einige Beispiele dazu, wie wir den Datenschutz, die Sicherheit und die Integrität fördern. Wir unternehmen Folgendes: Konten und Aktivität verifizieren, Verstöße gegen unsere Nutzungsbedingungen oder Richtlinien zu ermitteln und zu verfolgen. In einigen Fällen werden die von uns zu Verstößen getroffenen Entscheidungen vom Oversight Board überprüft. Bei der Überprüfung unserer Entscheidungen verwendet das Oversight Board möglicherweise uns zur Verfügung stehende Informationen. Mehr dazu, wie das Oversight Board Informationen verarbeitet: Verdächtige Aktivitäten untersuchen, Schädliches oder rechtswidriges Verhalten erkennen, verhindern und bekämpfen, Spam und andere negative Erlebnisse aufdecken und verhindern, Erkennen, wenn jemand Hilfe benötigt und Unterstützung anbieten, Bedrohungen unseres Personals bzw. Eigentums aufdecken und unterbinden, Die Integrität unserer Produkte wahren. Mehr dazu, was wir unternehmen, um Meta

zu einem sicheren Ort für alle zu machen. Bereitstellung von Messungs- und Analysediensten sowie Unternehmens-Services: Um Messungs- und Analysedienste bereitzustellen, verwenden wir die Informationen, die wir über dich erheben, in all deinen Konten auf unseren Produkten. Unsere Messungs- und Analysedienste unterstützen unsere Partner dabei, u. a. Folgendes zu verstehen: Wie viele Menschen ihre Inhalte, wie u. a. Beiträge, Videos, Facebook-Seiten, Inserate, Shops und Werbeanzeigen, sehen und mit ihnen interagieren (einschließlich derjenigen, die über Apps gezeigt werden, die das Meta Audience Network nutzen), Wie Nutzer mit ihren Inhalten, Websites, Apps und Diensten interagieren, Welche Personengruppen mit ihren Inhalten interagieren bzw. ihre Dienste nutzen. Kommunikation mit dir: Wir kommunizieren mit dir auf verschiedene Arten. Zum Beispiel: Wir senden dir Nachrichten zu den Produkten, von denen wir wissen, dass du sie nutzt, an die mit deinem Konto registrierte E-Mail-Adresse, Je nach deinen Einstellungen senden wir dir Marketingmitteilungen zu Produkten, die dir gefallen könnten, Basierend auf bestimmten Faktoren (z. B. wie du unsere Produkte nutzt) bitten wir dich, an Forschung teilzunehmen, Wir informieren dich über unsere Richtlinien und Nutzungsbedingungen, Wenn du uns bei Fragen kontaktierst, senden wir unsere Antwort an deine E-Mail-Adresse, Wir ermöglichen die Kommunikation des Support-Teams mit dir, wenn du uns entweder direkt oder über einen Dritten mitgeteilt hast, dass du Fragen oder Anliegen bezüglich unserer Produkte hast. Forschung und Innovation für soziale Zwecke: Wir forschen und innovieren, um Menschen auf der ganzen Welt zu helfen. Unsere Ziele sind u. a.: Einen Beitrag für soziale Zwecke und Bereiche von öffentlichem Interesse leisten, Die Technologie vorantreiben, Sicherheit, Gesundheit und Wohlbefinden verbessern. Hier sind ein einige Beispiele für unsere Forschungen: Wir analysieren Informationen dazu, wohin Personengruppen in Krisensituationen gehen. Dies unterstützt Hilfsorganisationen dabei, Hilfsmittel und Unterstützung an die richtigen Orte zu bringen. Wir arbeiten mit unabhängigen Forschern zusammen, um bessere Einblicke in die Auswirkungen zu erlangen, die soziale Medien auf Wahlen und demokratische Prozesse haben können, Gemeinsam mit Wissenschaftlern und Branchenexperten haben wir an der Verbesserung von Internetzugang und qualität in ländlichen Gebieten gearbeitet, Wir unterstützen die Forschung in Bereichen wie künstliche Intelligenz und maschinelles Lernen, um beispielsweise COVID-19-Prognosemodelle zu entwickeln. Informationen über unsere Produkte hinweg nutzen: Wir nutzen Informationen über deine Konten unserer Produkte hinweg, um: Werbeanzeigen für dich und andere zu personalisieren, Leistung dieser Werbeanzeigen zu messen, stärker personalisierte Funktionen, Inhalte und Vorschläge über unsere Produkte hinweg bereitzustellen. Einige Beispiele: Personen mit einer höheren Genauigkeit zu zählen und zu verstehen, wie sie unsere Produkte nutzen, für deine und die Sicherheit anderer zu sorgen. Wenn du deine Kontenübersicht einrichtest, nutzen wir deine Informationen auch, um verknüpfte Funktionen anzubieten und deine Erfahrungen über Konten hinweg zu verbessern. Darum nutzen wir Informationen über Geräte hinweg: **Wir nutzen deine Informationen über Geräte hinweg unter anderem aus dem Grund, um dir eine stärker personalisierte Erfahrung bieten zu können.** So zeigen wir dir beispielsweise eine Werbeanzeige auf deinem Telefon und später klickst du möglicherweise über deinen Laptop auf die Anzeige und kaufst das Produkt. Indem wir diese Informationen über deine Geräte hinweg zusammenführen, können wir verstehen, welche Werbeanzeigen für dich relevant sind, und Unternehmen helfen, die Effektivität ihrer Werbung zu messen. Manuelle Überprüfung: Wann wir manuelle Überprüfung verwenden: Unsere Überprüfer helfen uns dabei, Sicherheit und Integrität für unsere Produkte zu fördern. Beispielsweise können unsere Überprüfer nach Inhalten Ausschau halten, die gegen unsere Nutzungsbedingungen und Richtlinien verstoßen, und diese entfernen. Inhalte, die unsere Nutzungsbedingungen und Richtlinien befolgen, bleiben erhalten. Ihre Arbeit ergänzt unsere Technologie, die Verstöße erkennt. Wenn unsere Algorithmen feststellen, dass jemand Hilfe benötigen könnte, kann ein Überprüfer dessen Post prüfen und gegebenenfalls Unterstützung anbieten. Wir nutzen unsere manuelle Überprüfung auch, um Inhalte zu analysieren, damit wir unsere Algorithmen so trainieren können, dass sie Inhalte auf dieselbe Weise prüfen wie eine Person. Dadurch wird unsere automatische Verarbeitung verbessert, was uns wiederum dabei hilft, unsere Produkte zu verbessern. Wer diese Informationen prüft: Unsere Überprüfer arbeiten bei Meta, Meta-Unternehmen oder einem vertrauenswürdigen Anbieter. Jeder Überprüfer, dem Zugriff auf deine Informationen gewährt wird, muss Datenschutz- und Sicherheitsstandards erfüllen. So personalisieren wir deinen Facebook-Feed: Dein Facebook-Feed ist individuell auf dich zugeschnitten. Wir ordnen die Inhalte, die du in deinem Feed sehen kannst, in einer bestimmten Reihenfolge an (bzw. weisen ihnen ein „Ranking“ zu). Erfahre mehr zu den verschiedenen Arten von Signalen, die wir für das Ranking verwenden. Wir schlagen dir auch Inhalte vor, die für dich relevant sind. Viele Faktoren beeinflussen die Inhalte, die du in deinem Feed siehst. Beispiele: Wenn deine Freunde, Kontakte oder Personen, die du kennen könntest, mit einer Facebook-Seite, einem Beitrag oder einem bestimmten Thema interagieren, können wir dir ähnliche Inhalte vorschlagen. Beispiel: Wenn dein Freund Ahmad einen Beitrag über Nationalparks kommentiert, können wir dir den Beitrag zu Nationalparks vorschlagen. Wenn du und andere mit derselben Gruppe, Facebook-Seite oder demselben Beitrag interagiert, können wir dir eine andere

Gruppe, Seite oder einen anderen Beitrag vorschlagen, mit der/dem sie interagieren. Beispiel: Wenn du und Sharmila derselben Gruppe von Katzenfreunden angehört und Sharmila eine Seite, auf der Schals verkauft werden, mit „Gefällt mir“ markiert, können wir dir die Schal-Seite vorschlagen. Wenn du kürzlich mit einem bestimmten Thema auf Facebook interagiert hast, können wir dir anschließend andere Beiträge vorschlagen, die mit diesem Thema zusammenhängen. Beispiel: Wenn du kürzlich einen Beitrag von einer Basketball-Seite mit „Gefällt mir“ markiert oder kommentiert hast, könnten wir dir andere Beiträge über Basketball vorschlagen. Je nachdem, wo du dich befindest und womit Personen in deiner Nähe auf Facebook interagieren, können dir Beiträge angezeigt werden. Beispiel: Wenn du dich in der Nähe eines Sportstadions befindest, können wir dir Spiele oder Veranstaltungen im Stadion vorschlagen. Erfahre mehr dazu, wie wir standortbezogene Informationen nutzen. Deine Aktivität in unseren Produkten: Beispiel: William schaut sich eine lokale Bäckerei auf Facebook an, also zeigen wir ihm später möglicherweise Werbeanzeigen für andere lokale Bäckereien auf Instagram. Deine Aktivität auf Websites und in Apps, abhängig von deinen Einstellungen: Beispiel: Jane kauft ein Paar Schuhe in einem Online-Schuhgeschäft. Das Geschäft teilt Janes Aktivitäten mit uns über unsere Business-Tools, die unseren Business-Tool-Nutzungsbedingungen unterliegen. Später sieht Jane eine Werbeanzeige auf Instagram für einen Rabatt auf ihren nächsten Schuhkauf bei diesem Online-Geschäft. Wenn sie keine weitere Werbung dieses Schuhgeschäfts angezeigt bekommen möchte, kann sie sie in ihren Werbekunden-Einstellungen ausblenden. Oder wenn sie von uns keine weitere Werbung basierend auf ihren Aktivitäten auf anderen Websites und Apps erhalten möchte, kann sie dies in ihren Werbeeinstellungen deaktivieren. Themen, die dich interessieren könnten: Beispiel: Jon hat mehrere Facebook-Seiten von berühmten Musikern mit „Gefällt mir“ markiert. Daher nehmen wir an, er interessiert sich für „Musik“. Basierend auf diesem Interesse, zeigen wir ihm möglicherweise Werbung für einen lokalen Plattenladen oder eine Online-Musikveröffentlichung. Deine Verbindungen: Beispiel: Fionas Freund hat einen Instagram-Account für eine örtliche Kunstmesse mit „Gefällt mir“ markiert. Basierend auf der Aktivität ihres Freundes/ihrer Freundin zeigen wir Fiona möglicherweise eine Werbeanzeige für eine Kunstmesse. Andere Gerätesignale, die wir erhalten: Wir erhalten verschiedene Arten von Gerätesignalen von verschiedenen Betriebssystemen. Dazu gehören **Bluetooth- oder WLAN-Verbindungen in der Nähe. IP-Adressen: IP-Adresse steht für „Internet-Protokoll-Adresse“**. Es handelt sich um eine Nummer, die einem Geräte (z. B. Telefon oder Computer) zugewiesen wurde, mit der es über das Internet kommunizieren kann. Diese Nummern werden gemäß Standardrichtlinien oder Protokollen zugewiesen. So wie du eine Adresse benötigst, um Briefe von deinen Freunden zu bekommen, benötigt dein Gerät eine IP-Adresse, um Informationen im Internet zu erhalten. Personalisieren von Werbeanzeigen für dich und andere: Beispiel: Marcus geht auf Reisen und möchte mit der Funktion „WLAN finden“ kostenloses, öffentliches WLAN am Flughafen finden. Er hat Ortungsdienste eingeschaltet, sodass wir ihn mithilfe seiner GPS-Informationen dabei unterstützen können, die relevantesten öffentlichen WLAN-Netzwerke zu finden. Wir nutzen diese Informationen außerdem, um ihm Werbung für lokale Unternehmen in der Nähe des Flughafens zu zeigen. Später schaltet Marcus Ortungsdienste aus, bevor er landet, damit wir seinen GPS-Informationen nicht mehr erheben. Im weiteren Verlauf seiner Reise öffnet er die Facebook-App, und wir können anhand der IP-Adresse, die wir erhalten, den aktuellen Standort von Marcus schätzen und ihm Werbung für Unternehmen in der Nähe zeigen. Unterstützung beim Schutz deines Kontos: Wir nutzen beispielsweise Informationen über die Standorte, von denen du dich normalerweise anmeldest, in Kombination mit anderen Informationen, um verdächtige Aktivitäten zu erkennen. Wenn wir einen Anmeldeversuch für dein Konto an einem neuen Standort feststellen, können wir prüfen, ob es sich wirklich um dich handelt. Informationen, die wir zu verschiedenen Personen bereitstellen: Zum Beispiel teilen wir möglicherweise einem Werbetreibenden mit, dass seine Anzeige von Frauen im Alter von 25–34 gesehen wurde, die in Madrid leben und sich für Softwareentwicklung interessieren. Bereitstellung stärker personalisierter Funktionen, Inhalte und Vorschläge über unsere Produkte hinweg Wir können beispielsweise: automatisch Registrierungsinformationen, wie z. B. deine Telefonnummer, von einem Meta-Produkt ausfüllen, wenn du ein Konto bei einem anderen Produkt erstellst, andere deinen Namen und dein Profilbild in unseren Produkten sehen und danach suchen lassen sowie mit dir kommunizieren lassen, alle Interaktionen zu Inhalten, die du auf über verschiedene Produkte hinweg gepostet hast, an einem Ort anzeigen. Verwendung deiner Informationen, wenn du deine Kontenübersicht einrichtest: Wenn du beispielsweise deinem Lieblingsteam auf Instagram folgst, können wir dir viel einfacher auf Facebook vorschlagen, der Seite dieses Teams zu folgen. Mehr dazu, wie wir Informationen über Konten hinweg nutzen, wenn du eine Kontenübersicht einrichtest. Wie werden deine Informationen auf Meta-Produkten bzw. mit integrierten Partnern geteilt? Auf Meta-Produkten: Erfahre mehr über die verschiedenen Fälle, in denen deine Informationen auf unseren Produkten geteilt werden können: **Personen und Konten, mit denen du Inhalte teilst bzw. kommunizierst. Wenn du unter Nutzung unserer Produkte Inhalte teilst bzw. kommunizierst, kannst du manchmal die Zielgruppe auswählen für die Inhalte, die du teilst.** Wenn du mit Personen oder

Unternehmen interagierst, können sie Folgendes sehen: Was du mit ihnen teilst: Die von dir ausgewählte Zielgruppe kann zum Beispiel sehen, wenn du: **einen von dir verfassten Beitrag teilst, ein Foto oder Video teilst, eine Story erstellst, einen Nachrichtenartikel postest, oder Informationen zu deinem Profil hinzufügst. Was du mit ihnen kommunizierst: Personen, mit denen du interagierst, können sehen, was du ihnen sendest.** Wenn du also einer Person oder einem Unternehmen eine Nachricht im Messenger oder auf Instagram sendest, kann diese Person bzw. dieses Unternehmen deine Nachricht lesen. Einige deiner Aktivitäten: Personen und Unternehmen können außerdem einige deiner Aktivitäten auf unseren Produkten sehen. Dies ist beispielsweise dann der Fall, wenn du: die Beiträge anderer kommentierst oder auf sie reagierst, mit Werbeanzeigen oder anderen gesponserten oder kommerziellen Inhalten interagierst, z. B. indem du sie kommentierst oder mit „Gefällt mir“ markierst, zulässt, dass Inhalte, die du in einem Shop über ein Produkt geteilt hast, unter unseren Produkten geteilt werden, die Story anderer Nutzer auf Facebook oder Instagram ansiehst, ein neues Meta-Gerät, wie Portal oder Ray-Ban Stories, mit deinem Konto verbindest. Wenn du aktiv bist: Auf einigen unserer Produkte stehen dir möglicherweise Einstellungen zur Verfügung, über die andere sehen können, wenn du auf unseren Produkten aktiv bist (Beispiel: „Aktiv-Status“). In einigen Fällen bieten wir auch Einstellungen an, die es anderen ermöglichen, zu sehen, wenn du in einem bestimmten Bereich unserer Produkte aktiv bist, z. B. in einem Nachrichten-Thread, einem Spiel oder einer Veranstaltung, oder wann du eines unserer Produkte zuletzt genutzt hast. So aktualisierst du deinen Aktiv-Status auf Facebook und im Messenger bzw. auf Instagram. Inhalte, die andere über dich (erneut) teilen: Wer deine Inhalte sehen oder (erneut) teilen kann: Personen in deiner Zielgruppe können deine Inhalte sehen und sie sowohl auf als auch außerhalb von unseren Produkten ggf. mit anderen außerhalb deiner Zielgruppe teilen. Wenn du zum Beispiel einen Beitrag mit bestimmten Freunden teilst oder ihnen eine Nachricht sendest, können sie diese(n) herunterladen, einen Screenshot davon erstellen oder ihn/sie mit jeder beliebigen Person auf, in oder außerhalb von unseren Produkten teilen. Wenn du einen Beitrag kommentierst oder auf ein Foto reagierst, kann jeder, der den Beitrag oder das Foto sehen kann, auch deinen Kommentar bzw. deine Reaktion sehen. Dies können auch Personen sein, mit denen du nicht vernetzt bist. Außerdem kann die Person, die den Beitrag geteilt hat, jederzeit ihre Zielgruppe ändern, nachdem du mit dem Beitrag interagiert hast. So können Informationen über dich geteilt werden: Nutzer unserer Produkte können Informationen über dich mit der von ihnen ausgewählten Zielgruppe teilen. Sie können z. B. ein Foto oder Video von dir in einem Beitrag, einem Kommentar, einer Story, einem Reel oder einer Nachricht teilen, dich in einem Beitrag oder in einer Story erwähnen, dich in einem Beitrag, einem Kommentar, einer Story oder an einem Standort markieren, Details über dich in einem Beitrag, in einer Story oder in einer Nachricht teilen. Wenn es dir unangenehm ist, was andere über dich auf unseren Produkten geteilt haben, kannst du jederzeit Beiträge und Stories melden. Öffentliche Inhalte: Welche Inhalte sind öffentlich? Einige deiner Informationen und Aktivitäten sind immer öffentlich. Dies umfasst u. a. deinen Namen, deinen Facebook- und Instagram-Benutzernamen, dein Profilbild sowie deine Aktivität auf öffentlichen Facebook-Seiten und in öffentlichen Gruppen. Für andere Inhalte kannst du die Einstellung „Öffentlich“ wählen (z. B. für Beiträge, Fotos oder Videos, die du in deinem Profil, in Stories oder Reels postest). Wer kann öffentliche Inhalte sehen? Wenn Inhalte öffentlich sind, können sie von jedem auf oder in unseren Produkten gesehen werden, in einigen Fällen auch außerhalb unserer Produkte, und zwar selbst dann, wenn derjenige kein Konto hat. Wenn du z. B. etwas auf dem Marketplace, auf einer öffentlichen Facebook-Seite oder auf einem öffentlichen Instagram-Konto kommentierst oder ein Rating oder eine Bewertung hinterlässt, ist dein Kommentar, dein Rating bzw. deine Bewertung für jeden sichtbar. Diese können in all unseren Produkten erscheinen oder von jedem gesehen werden, auch außerhalb unserer Produkte. Wo können öffentliche Inhalte geteilt werden? Wir, du und Nutzer unserer Produkte können öffentliche Inhalte (wie dein Profilbild oder Informationen, die du auf einer Facebook-Seite oder auf einem öffentlichen Instagram-Konto teilst) an jeden auf, in oder außerhalb von unseren Produkten senden. Nutzer können sie beispielsweise in einem öffentlichen Forum teilen, oder sie können in Suchergebnissen im Internet erscheinen. Auf öffentliche Inhalte kann auch über Dienste Dritter zugegriffen werden bzw. sie können über diese gesehen, (erneut) geteilt oder heruntergeladen werden. Dies sind Dienste wie: Suchmaschinen, APIs, Medien wie das Fernsehen, andere mit unseren Produkten verbundene Apps und Websites. Mit integrierten Partnern: Du kannst wählen, ob du dich mit integrierten Partnern, die unsere Produkte nutzen, verbinden willst. Wenn du dies tust, erhalten diese integrierten Partner Informationen über dich und deine Aktivität. Diese integrierten Partner können immer auf die Informationen zugreifen, die auf unseren Produkten öffentlich sind. Weitere Infos zu sonstigen Informationen, die sie erhalten, und dazu, wie sie mit deinen Informationen umgehen: Wenn du das Produkt bzw. den Dienst eines integrierten Partners nutzt. Informationen, die sie automatisch erhalten: Wenn du die Produkte oder Dienste eines integrierten Partners nutzt, kann dieser auf Folgendes zugreifen: Was du über diese Produkte oder Dienste postest oder teilst, Wofür du ihre Dienste nutzt, Informationen durch bzw. über das von dir genutzte Gerät. Beispiele dazu, in welchen Fällen integrierte Partner deine Informationen

unter Umständen erhalten. Informationen, die sie mit einer Berechtigung von dir erhalten: Manchmal bitten dich diese integrierten Partner um deine Einwilligung, auf bestimmte zusätzliche Informationen von deinem Facebook-, Instagram- oder Messenger-Konto zuzugreifen. In ihrer Anfrage erläutern sie, auf welche Informationen sie zugreifen möchten. Du kannst dann entscheiden, ob du sie teilen möchtest. Auf Facebook betrifft dies u. a. deine E-Mail-Adresse, deine Heimatstadt oder deinen Geburtstag. Auf Instagram umfasst dies Inhalte wie Fotos und Videos, die du über dein Konto geteilt hast, als das Konto auf privat eingestellt war. Dies geschieht, wenn du deine Freundesliste teilst bzw. wenn deine Freunde ihre Freundesliste teilen. Wir protokollieren automatisch, wenn du von einem integrierten Partner eine Anfrage für den Zugriff auf deine Informationen erhältst. Diese Anfragen für den Zugriff unterscheiden sich vom Zugriff durch Apps und Websites, den du in deinen Facebook- oder Instagram-Einstellungen für Werbeanzeigen oder in den Einstellungen deines Mobilgeräts verwaltest. So lange können sie auf deine Informationen zugreifen: Apps oder Websites bei denen du dich mit Facebook Login angemeldet hast bzw. die mit deinem Instagram-Konto verknüpft sind, können auf deine nichtöffentlichen Informationen auf Meta-Produkten zugreifen, es sei denn, wir haben den Eindruck, dass du die App oder Website 90 Tage lang nicht genutzt hast. Hinweis: Selbst wenn der Zugriff einer App auf deine Daten abgelaufen ist, kann sie noch Informationen gespeichert haben, die du zuvor mit ihr geteilt hast. Wir empfehlen dir, deine Einstellungsseite „Apps und Websites“ regelmäßig aufzurufen, um zu überprüfen, welche Apps und Websites über Facebook Login oder Instagram weiterhin Zugriff auf deine Informationen haben. Wenn du in einem Produkt oder Dienst eines integrierten Partners mit Inhalten anderer Personen interagierst. Integrierte Partner erhalten Informationen über deine Aktivität, wenn du mit anderen Facebook-, Instagram- oder Messenger-Nutzern interagierst, während sie das Produkt oder den Dienst des integrierten Partners nutzen. Ein Spieler schaltet beispielsweise mit Hilfe einer Partner-App einen Facebook-Livestream. Anschließend kommentierst du diesen Livestream. Der App-Entwickler erhält dann Informationen zu deinem Kommentar. So gehen integrierte Partner mit deinen Informationen um: Integrierte Partner behandeln die Informationen, die du mit ihnen teilst, gemäß ihren eigenen Nutzungsbedingungen und Richtlinien und nicht gemäß denen von Meta. Du kannst ihre Datenrichtlinie auf/in ihrer jeweiligen Website bzw. App nachlesen. Darin erfährst du, wie sie deine Informationen erhalten und verarbeiten. In einigen Fällen setzen sie für den Empfang und die Verarbeitung deiner Informationen einen gesonderten Dienstleister ein. Zielgruppe auswählen: Auf Facebook kann sich die Zielgruppe folgendermaßen zusammensetzen: Die Öffentlichkeit, einschließlich Personen mit und ohne Facebook-Konto, Deine Freunde und andere Kontakte, z. B. die Freunde von Personen, die du markierst, Eine benutzerdefinierte Liste von Personen, Du selbst, Die Mitglieder einer einzelnen Community, etwa einer Gruppe. Auf Instagram kannst du die Zielgruppe für das, was du teilst, festlegen, indem du zwischen einem privaten oder öffentlichen Konto wählst. Bei einem privaten Konto können nur von dir genehmigte Abonnenten sehen, was du teilst. Bei einem öffentlichen Konto können deine Beiträge und andere Inhalte auf Instagram von jedem auf oder außerhalb von unseren Produkten gesehen werden, also auch, wenn er/sie kein Konto hat. Du kannst die Zielgruppe für deine Inhalte einschränken, indem du einzelne Konten blockierst, sodass diese deine Inhalte nicht länger sehen können. Außerdem kannst du eine Liste deiner engen Freunde für bestimmte Inhalte erstellen, die nur Personen auf dieser Liste sehen können. Suchmaschinen: Du kannst in deinen Privatsphäre-Einstellungen angeben, ob Suchmaschinen außerhalb von Facebook auf dein Profil verlinken können. Andere öffentliche Inhalte – z. B. Posts, bei denen deine Zielgruppe auf öffentlich eingestellt ist, oder Posts auf öffentlichen Seiten oder Konten – sind jedoch möglicherweise weiterhin über Suchmaschinen zugänglich, je nach Einstellung des jeweiligen Kontos. Unsere Partner Unternehmen und Personen können unsere Produkte nutzen, um ihre Produkte und Dienste zu bewerben, zu vertreiben oder zu unterstützen. Wenn sie unsere Produkte nutzen, nennen wir sie unsere Partner. Zu unseren Produkten gehören Business-Tools und andere Technologien, mit denen Unternehmen ihre Produkte und Dienstleistungen bewerben oder unterstützen oder feststellen und messen können, wie ihre Dienstleistungen genutzt werden und wie gut ihre Anzeigen funktionieren. Beispielsweise können sie eines unserer Business-Tools, das Meta-Pixel, auf ihrer Website platzieren. Oder sie verwenden die Meta Audience Network-Tools, um mit ihren Apps Geld zu verdienen, indem sie Werbeanzeigen von Unternehmen zeigen, die Werbung auf Facebook schalten. Zu unseren Produkten gehören außerdem Technologien, mit denen über unsere Produkte eine Verbindung zu unseren Partnern hergestellt werden kann. Denkbar ist beispielsweise, dass du dich über Facebook Login bei deren App oder Website anmeldest. Oder du spielst deren Spiel auf Facebook. Das nennen wir eine Integration, denn du kannst spielen, ohne unsere App zu verlassen. Wir nennen die Partner, die diese integrierten Tools nutzen, unsere integrierten Partner. Hier sind ein paar Beispiele: Werbetreibende, Unternehmen, die die Effektivität der Werbeanzeigen messen und Berichte erstellen, Unternehmen und Personen, die unsere Produkte verwenden, um Waren und Dienstleistungen zu verkaufen oder anzubieten. Publisher (wie eine Website oder App) und deren Geschäftspartner, App-Entwickler, Spieleentwickler. Fälle, in denen integrierte Partner unter Umständen deine Informationen

erhalten: Möglicherweise nutzt du deinen Facebook Login zum Beispiel für ein Online-Spiel mit deinen Facebook-Freunden. Der Spieleentwickler erhält automatisch Informationen zu deinen Aktivitäten im Spiel. Fälle, in denen integrierte Partner unter Umständen deine Informationen erhalten: Oder du nutzt vielleicht den „Gefällt mir“-Button von Facebook auf einem Artikel, der auf einer Nachrichten-Website veröffentlicht wurde. Der Websiteentwickler erhält automatisch Informationen zu deiner „Gefällt mir“-Angabe für seinen Artikel. Freundeslisten teilen: Wenn du deine Freundesliste teilst: Wenn du den Facebook Login nutzt, um dich bei einer App anzumelden, fordert der App-Entwickler möglicherweise Zugriff auf deine Freundesliste bei Facebook. Wenn du dem App-Entwickler die Berechtigung erteilst, diese Listen einzusehen, geschieht Folgendes: Er kann eine Liste deiner Facebook-Freunde, die dieselbe App nutzen und der App die Berechtigung zum Zugriff auf ihre Freundesliste erteilt haben, einsehen und auf sie zugreifen. Er hat dadurch jedoch keinen Zugriff auf nicht öffentliche Informationen über deine Freunde oder Abonnenten. Hinweis: Der App-Entwickler erhält weitere Informationen über deine Freunde, wenn diese sie selbst teilen. Dies können sie tun, indem sie die Informationen direkt bereitstellen oder den Entwickler dazu berechtigen, auf Informationen ihres Kontos zuzugreifen. Du erscheinst in Freundeslisten, die deine Facebook-Freunde mit derselben App teilen können. Du kannst diese Berechtigung bzw. die komplette App entfernen, wenn du zu einem späteren Zeitpunkt entscheidest, dass du deine Freundesliste nicht mit einer App teilen oder nicht auf anderen Freundeslisten erscheinen möchtest, die mit dieser App geteilt werden. Wenn deine Freunde ihre Freundesliste teilen: Deine Freunde entscheiden sich möglicherweise dazu, ihre Freundesliste mit App-Entwicklern über den Facebook Login zu teilen. Sie können jedoch über den Facebook Login keine nicht öffentlichen Informationen über dich weitergeben. Wie teilen wir Informationen mit Partnern, Anbietern, Dienstleistern und Dritten? **Wir verkaufen keine deiner Informationen an irgendjemanden und werden das auch in Zukunft niemals tun.** Außerdem verpflichten wir Partner und Dritte, Regeln dazu einzuhalten, wie sie die Informationen, die wir bereitstellen, nutzen und offenlegen dürfen und wie nicht. Weitere Einzelheiten dazu, an wen wir Informationen weitergeben: Partner, Werbetreibende und Audience Network-Publisher, Werbetreibende. Wir stellen Werbetreibenden Berichte über die Anzahl und Arten von Personen bereit, die sich ihre Werbeanzeigen ansehen bzw. mit diesen interagieren. Diese Berichte enthalten Informationen über die allgemeine Demografie sowie die Interessen der Personen, die mit einer Werbeanzeige des jeweiligen Werbetreibenden interagiert haben. Dadurch können Werbetreibende ihre Zielgruppe besser verstehen. Ein Beispiel ansehen. Meta stellt Werbetreibenden und ihren Geschäftspartnern auch Informationen zu Folgendem bereit: Werbeanzeigen, mit denen Personen interagiert haben (falls zutreffend), Wann Personen mit Werbeanzeigen interagiert haben, Wo die Werbeanzeige gezeigt wurde (z. B. auf Instagram oder auf Facebook). Wir teilen mit diesen Werbetreibenden und ihren Geschäftspartnern jedoch keine Informationen, die für sich genommen dazu verwendet werden können, dich zu kontaktieren oder identifizieren (wie z. B. dein Name oder deine E-Mail-Adresse), es sei denn, du gibst uns deine Einwilligung dazu. Audience Network-Publisher und ihre Geschäftspartner: Mit dem Meta Audience Network können Werbetreibende Anzeigen bei uns schalten, die in Apps außerhalb von Meta veröffentlicht werden. Um dich dabei zu unterstützen, deine Werbeanzeigen in ihren Apps zu zeigen, teilen wir Informationen mit Publishern, die das Audience Network nutzen, sowie mit Geschäftspartnern, die diese Nutzung ermöglichen. Wir teilen beispielsweise folgende Informationen: Wie viele Personen sich Werbeanzeigen in Publisher-Apps ansehen bzw. mit ihnen interagieren, Informationen im Zusammenhang mit einem oder als Reaktion auf einen Antrag eines Publishers, eine Werbeanzeige in seiner App zu zeigen. Wir teilen mit diesen Publishern und ihren Geschäftspartnern jedoch keine Informationen, die für sich genommen dazu verwendet werden können, dich zu kontaktieren oder identifizieren (wie z. B. dein Name oder deine E-Mail-Adresse), es sei denn, du gibst uns deine Einwilligung dazu. Partner, die unsere Analysedienste nutzen: Menschen setzen auf unsere Produkte, wie Unternehmenskonten, professionelle Tools und Facebook-Seiten, um ihre Unternehmen zu betreiben und zu bewerben. Unternehmen nutzen unsere Analysedienste, um mehr darüber zu erfahren, wie Nutzer ihre Inhalte und Features verwenden. Wir erhalten Informationen darüber, wie Nutzer mit ihren Beiträgen, Inseraten, Facebook-Seiten, Videos, Shops oder sonstigen Inhalten auf und außerhalb von unseren Produkten interagieren. Anschließend stellen wir ihnen diese Informationen in aggregierten Berichten zur Verfügung, damit sie sehen können, wie gut die Performance ihrer Inhalte ist. Diese Berichte fassen z. B. Informationen hierzu zusammen: **Wie viele Personen mit ihren Inhalten interagiert haben, Allgemeine Demografie und Interessen der Personen, die mit ihnen interagiert haben Partner, die bei uns werben, erhalten auch andere Informationen.** Lies unsere Richtlinie dazu, wie wir Informationen mit Werbetreibenden teilen. Partner, die Waren und Dienstleistungen in unseren Produkten und auf unseren Plattformen für E-Commerce-Dienste anbieten. Wenn du freiwillig eine Transaktion durchführst oder anderweitig freiwillig Informationen mit einem Verkäufer, Creator, einer Spendenaktion, Wohltätigkeitsorganisation, einem Anbieter für Zahlungsdienste oder einer Plattform für E-Commerce-Dienste[42] teilst, geben wir Informationen an diese und andere Anbieter weiter, die in deren Namen handeln. Je nachdem, wie du mit ihnen

interagierst, erhalten sie: Informationen, um deine Transaktion abzuschließen, wie Bestell-, Zahlungs-, Kontakt- und Versandinformationen, Informationen, die dazu beitragen, die Sicherheit der Transaktion zu gewährleisten, wie Informationen über dein Gerät oder deine Verbindung, Jegliche Informationen, die nach geltenden Vorschriften erforderlich sind, Sonstige Informationen, die du entscheidest, mit ihnen zu teilen. Wenn du beispielsweise einen Kauf von einem Instagram-Shop über den Checkout tätigt, erhält der Shop Informationen, um deine Transaktion abzuschließen. Dies kann deine bestellten Artikel, deine Kontaktdaten und deine Versandinformationen umfassen. Wenn der Shop einen Anbieter für Zahlungsdienste (z. B. PayPal) nutzt, um die Transaktion durchzuführen, erhält der Anbieter den Transaktionsbetrag, eine Beschreibung der Transaktion (diese erscheint auf deiner Kreditkartenabrechnung) und Informationen zu deiner Zahlungskarte, wie Name des Karteninhabers, Kartenummer, Ablaufdatum und Rechnungsadresse. Mehr zu Zahlungen auf Instagram.

Integrierte Partner: Wenn du Produkte oder Dienstleistungen von integrierten Partnern freiwillig nutzt, erhalten diese Informationen über dich und deine Aktivität.

Anbieter: Anbieter für Mess- und Marketinglösungen: Anbieter für Mess- und Marketinglösungen sind Unternehmen, die Meta und seinen Werbekunden Unterstützung im Zusammenhang mit Marketing anbieten. Beispielsweise kaufen sie in unserem Namen Werbeanzeigen, stellen Marktforschung bereit und messen die Effektivität unserer Kampagnen. Diese Anbieter unterstützen auch die Werbung unserer Partner.

Anbieter für Messlösungen: Wir erstellen nicht jeden Messungs- und Analysebericht selbst. Wir arbeiten mit Anbietern für Messlösungen zusammen, die Berichte erstellen, die unsere Partner, z. B. Werbekunden, dabei unterstützen, zu verstehen, wie erfolgreich ihre Inhalte und Werbeanzeigen sind, wer mit ihnen interagiert und ob Personen eine Handlung ausgeführt haben, nachdem sie ihre Werbeanzeige gesehen haben. Wir teilen Informationen (z. B. ob Personen eine Werbeanzeige gesehen oder mit ihr interagiert haben) mit unseren Anbietern für Messlösungen, die sie zusammenfassen, um ihre Berichte bereitzustellen. Ein Beispiel ansehen.

Anbieter für Marketinglösungen: Wir teilen Informationen über dich mit Unternehmen, die uns bei der Vermarktung unseres Unternehmens und unserer Produkte, bei der Messung der Effektivität unserer eigenen Marketingkampagnen und bei der Werbeforschung unterstützen. Beispielsweise teilen wir deine Geräte-ID oder andere Kennungen mit Werbungsanbietern, damit sie uns dabei unterstützen, dir Anzeigen auszuliefern, die für deine Interessen möglichst relevant sind. Mehr dazu, wie Anbieter unsere Marketing- und Werbemaßnahmen unterstützen.

Dienstleister: Dienstleister erbringen uns Dienstleistungen, die uns bei der Bereitstellung unserer Produkte für dich unterstützen. Wir teilen die uns über dich zur Verfügung stehenden Informationen mit ihnen, um u. a. nachstehende Dienstleistungen zu erhalten: Untersuchung verdächtiger Aktivitäten, Aufdeckung und Unterbindung von Bedrohungen unseres Personals bzw. Eigentums, Durchführung von Zahlungen, Bereitstellung von Kundensupport, Verbesserung der Funktionalität unserer Produkte, Erbringung technischer Infrastrukturdienstleistungen, Analyse der Nutzung unserer Produkte, Durchführung von Studien und Umfragen, Vermarktung und Bewerbung unserer Produkte, Analyse der Effektivität unserer Werbeanzeigen.

Dritte: Externe Forscher: Wir stellen externen Forschern Informationen bereit. Sie verwenden diese Informationen, um Studien durchzuführen, die Forschung und Innovation vorantreiben, und um den Schutz, die Sicherheit und die Integrität zu fördern. Mit den Studien soll u. a. Folgendes unterstützt werden: Unser Unternehmen bzw. unsere Mission, Soziale Zwecke, Technologischer Fortschritt, Schutz und Sicherheit auf unseren Produkten, Öffentliches Interesse, Gesundheit und Wohlbefinden. Wenn wir Daten an externe Forscher weitergeben, stellen wir sicher, dass die Privatsphäre unserer Nutzer geschützt ist. Mehr zu den von uns unterstützten datenschutzkonformen Studien. In anderen Fällen teilen wir Informationen mit Dritten. Außerdem teilen wir Informationen mit Dritten als Reaktion auf rechtliche Anfragen, um geltendes Recht einzuhalten oder um Schaden zu verhindern. Die Richtlinie lesen. Und wenn wir unser gesamtes Unternehmen bzw. Teile davon an jemand anderen verkaufen oder übertragen, können wir gemäß geltendem Recht deine Informationen im Rahmen dieser Transaktion an den neuen Eigentümer weitergeben.

Allgemeine demografische Angaben und Interessen: Beispiel: Ein Fahrradgeschäft erstellt eine Seite auf Facebook und möchte eine Anzeige schalten, um Personen in Atlanta, die sich für Radfahren interessieren, als Zielgruppe zu erreichen. Wir ermitteln beispielsweise anhand der Tatsache, ob jemand eine Seite über Fahrräder mit „Gefällt mir“ markiert hat, ob diese Person zur Zielgruppe passt. Dann könnten Personen in dieser Zielgruppe die Anzeige des Fahrradgeschäfts sehen. Du siehst, welche „Interessen“ dir in deinen Werbepräferenzen zugeordnet sind, und kannst sie entfernen, wenn du möchtest. Das Fahrradgeschäft kann dann Berichte mit aggregierten Statistiken zu der Zielgruppe aufrufen, die seine Anzeigen sehen, und die Performance der Anzeigen ermitteln. Die Berichte zeigen dem Werbetreibenden z. B. Statistiken an, die besagen, dass der Großteil der Personen, die die Anzeige gesehen oder darauf geklickt haben: Frauen waren, Zwischen 25 und 34 Jahre alt waren, Auf ihrem Telefon auf die Anzeige geklickt haben. Wenn du uns möglicherweise Erlaubnis erteilst: Beispiel: Du forderst möglicherweise mehr Informationen von einem Unternehmen an, indem du auf seine Werbeanzeige in deinem Facebook-Feed klickst und ein

Formular mit deinem Namen und Kontaktinformationen absendest. Dann erhält der Werbetreibende die von dir bereitgestellten Informationen. Transaktionen, die du vielleicht tätigt: Abonnement von Premium-Inhalten, Kaufen, Verkaufen oder Nutzen von Produkten, Kaufen, Verkaufen oder Nutzen von Dienstleistungen, Für wohltätige Zwecke spenden. Plattformen für E-Commerce-Dienste: Plattformen für E-Commerce-Dienste bieten eine Reihe von E-Commerce-Dienstleistungen an, darunter: Zahlungen, Marketing, Versand, Kundeninteraktionstools. So nutzen Anbieter von Messungen Informationen, um Berichte zu erstellen: Beispielsweise bittet ein Werbetreibender einen Anbieter für Messungen um Hilfe, um die Auswirkung seiner Werbeanzeigen auf Facebook auf die Verkäufe zu ermitteln. Der Anbieter für Messungen vergleicht die Informationen von uns zu Klicks auf die Facebook-Anzeigen des Werbetreibenden mit den Informationen des Werbetreibenden zu Produktkäufen. Daraufhin erstellt der Anbieter für Messungen aggregierte Berichte, die dem Werbetreibenden die Leistung seiner Anzeigen darstellen, und stellt sie zur Verfügung. So unterstützen Anbieter unsere Marketing- und Werbemaßnahmen: Beispielsweise übernehmen Anbieter folgende Aufgaben: Sie liefern unsere Werbeanzeigen im Internet aus, unter anderem auf mobilen, Desktop- und verbundenen Fernsehgeräten. Sie tracken und kategorisieren deine Online-Aktivitäten und Aktivitäten in der mobilen App. Sie stellen uns Informationen zu deinen Interessen sowie Community- und Werbungsinteraktionen bereit. Mithilfe dieser Anbieter können wir ermitteln, wer unsere Werbung für seine Interessen besonders relevant finden könnte und welches unserer Produkte für dich von Interesse sein könnte. Diese Informationen können zur Personalisierung verwendet werden, welche unserer Anzeigen dir gezeigt werden. Anbieter nutzen diese Informationen außerdem, um die Reaktion auf unsere Marketingmaßnahmen und die Wirksamkeit unserer Werbung zu messen. Wie arbeiten die Meta-Unternehmen zusammen? Wir sind Teil der Meta-Unternehmen, die Produkte der Meta-Unternehmen bereitstellen. Zu den Produkten der Meta-Unternehmen zählen alle Meta-Produkte, die in dieser Richtlinie behandelt werden, sowie weitere Produkte wie u. a. WhatsApp und Novi. Wir teilen die von uns erhobenen Informationen sowie die Infrastruktur, die Systeme und die Technologie mit den anderen Meta-Unternehmen. Erfahre mehr dazu, wie wir Informationen in andere Länder übermitteln. Außerdem verarbeiten wir Informationen, die wir über dich von anderen Meta-Unternehmen erhalten, gemäß deren Nutzungsbedingungen und Richtlinien und soweit dies nach anwendbarem Recht zulässig ist. In einigen Fällen fungiert Meta als Dienstleister für andere Meta-Unternehmen. Wir handeln in deren Auftrag und im Einklang mit deren Anweisungen und Nutzungsbedingungen. Warum wir Informationen innerhalb der Meta-Unternehmen weitergeben: Meta-Produkte geben Informationen an andere Meta-Unternehmen weiter: um Schutz, Sicherheit und Integrität zu fördern sowie das anwendbare Recht einzuhalten, um Angebote, Werbeanzeigen und andere gesponserte oder kommerzielle Inhalte zu personalisieren, um Features und Integrationen zu entwickeln und bereitzustellen, um herauszufinden, wie Personen Produkte der Meta-Unternehmen nutzen und mit ihnen interagieren. Warum wir Informationen innerhalb der Meta-Unternehmen weitergeben: Förderung von Sicherheit und Integrität sowie Einhaltung der geltenden Gesetze. Wir geben beispielsweise Informationen an Meta-Unternehmen weiter, die finanzielle Produkte und Dienstleistungen anbieten, um ihnen dabei zu helfen, Schutz, Sicherheit und Integrität zu fördern und das anwendbare Recht einzuhalten. Dazu gehören: Einhalten ihrer rechtlichen Pflichten, Helfen, für deine und die Sicherheit anderer zu sorgen, Durchführen einer Kontoverifizierung, Untersuchen verdächtiger Aktivitäten, Erstellen von Analysen. Für diese Zwecke geben wir möglicherweise deinen Namen, deine E-Mail-Adresse, mit wem du befreundet bist und andere Kontoinformationen innerhalb der Meta-Unternehmen weiter. Entwicklung und Bereitstellung von Funktionen und Integrationen: Beispiel: Wenn sie in deinem Land verfügbar sind, kannst du bestimmte Integrationen nutzen, die deine WhatsApp-Erfahrung mit anderen Produkten der Meta-Unternehmen verbinden. Dank diesen Integrationen kannst unter anderem: dein Facebook Pay-Konto nutzen, um Zahlungsvorgänge über WhatsApp zu tätigen, mit deinen Freunden auf anderen Produkten der Meta-Unternehmen chatten, wie zum Beispiel Portal, indem du dein WhatsApp-Konto verknüpfst. Wir teilen auch Informationen mit Meta-Unternehmen, um Innovation zu unterstützen. So können deine Videos beispielsweise dabei helfen, unsere Produkte zu trainieren, damit sie Objekte, z. B. Bäume, oder Aktivitäten, z. B. ein Hund, der einen Ball jagt, erkennen. Diese Technologie hilft uns dabei, künftig neue Produkte oder Funktionen anzubieten. Verstehen, wie Personen unsere Produkte nutzen: Wir zählen individuelle Nutzer, monatlich aktive Nutzer und täglich aktive Nutzer unserer Produkte. Dank dieser Informationen erhalten wir Einblicke in die Community, die unsere Produkte nutzt, und können wichtige Trends zur Nutzung unserer Produkte öffentlich teilen. Was ist unsere Rechtsgrundlage für die Verarbeitung deiner Daten? Was sind deine Rechte? Nach geltendem Datenschutzrecht benötigen Unternehmen eine Rechtsgrundlage zur Verarbeitung von Daten. Mit „Verarbeitung personenbezogener Daten“ meinen wir die Arten, auf die wir deine Informationen so erfassen, verwenden und teilen, wie wir es in den anderen Abschnitten dieser Richtlinie oben beschrieben haben. Was ist unsere Rechtsgrundlage? Wir stützen uns bei der Verarbeitung deiner Informationen für die in dieser Datenrichtlinie beschriebenen Zwecke auf verschiedene Rechtsgrundlagen. Je nach den Umständen stützen wir uns

auf unterschiedliche Rechtsgrundlagen, wenn wir dieselben Informationen für verschiedene Zwecke verarbeiten. Für jede der nachstehend aufgeführten Rechtsgrundlagen erläutern wir, warum wir deine Informationen verarbeiten. Je nachdem, welche Rechtsgrundlage wir nutzen, stehen dir außerdem bestimmte Rechte zu. Diese haben wir hier erläutert. Dir steht unabhängig davon, welche Rechtsgrundlage Anwendung findet, immer das Recht auf Auskunftserteilung, Berichtigung bzw. Löschung deiner Informationen zu. Um deine Rechte auszuüben, rufe den Abschnitt „Was sind deine Rechte?“ auf. Wir verarbeiten Informationen für die folgenden Rechtsgrundlagen: Erfüllung eines Vertrags: Wir verarbeiten deine Informationen, die zur Erfüllung unserer Verträge mit dir erforderlich sind. Dazu gehört die Bereitstellung der Dienste, die in den Facebook-Nutzungsbedingungen, den Instagram-Nutzungsbedingungen, den Ergänzenden Oculus-Nutzungsbedingungen, den Ergänzenden Portal-Nutzungsbedingungen und den Ergänzenden Facebook View-Nutzungsbedingungen, zusammen die „Nutzungsbedingungen“, dargelegt sind. Einwilligung: Wir verarbeiten deine Informationen, wenn du uns deine Einwilligung erteilst. Du kannst uns beispielsweise gestatten, dir personalisierte Werbeanzeigen zu zeigen, die auf Informationen basieren, die uns Werbetreibende und andere Partner zu deinen Aktivitäten auf ihren Websites und in ihren Apps sowie zu bestimmten Offline-Interaktionen (z. B. Käufe) bereitstellen. Du kannst deine Einwilligung jederzeit widerrufen. Berechtigtes Interesse: Wir verarbeiten deine Informationen so, wie es für unsere berechtigten Interessen bzw. die von anderen erforderlich ist. Zu unseren Interessen zählen u. a. die Bereitstellung eines innovativen, personalisierten, sicheren und profitablen Dienstes für unsere Nutzer und Partner und die Reaktion auf rechtliche Anfragen. Wir verarbeiten deine Informationen jedoch nicht, wenn deine Interessen oder Grundrechte und Grundfreiheiten unsere überwiegen. Lebenswichtiges Interesse: Wir verarbeiten Informationen, wenn dies deinem Schutz dient oder Schäden verhindert, wie z. B., wenn wir dein Leben oder das Leben von jemand anderem retten. Rechtliche Verpflichtung: Wir verarbeiten Informationen so, wie es für uns erforderlich ist, um eine rechtliche Pflicht zu erfüllen. Öffentliches Interesse: Wir verarbeiten Informationen so, wie es im öffentlichen Interesse erforderlich ist, wie z. B., wenn wir Studien durchführen oder den Schutz, die Sicherheit und die Integrität fördern. Gemäß DSGVO und anderen relevanten Datenschutzgesetzen stehen dir folgende Rechte zu: Auskunftsrecht und Recht auf korrekte Informationen, Recht auf Widerruf der Einwilligung, Recht auf Übertragbarkeit deiner Informationen, Recht auf Herunterladen deiner Informationen, Recht auf Löschung von Informationen, Widerspruchsrecht, Recht auf Einreichen einer Beschwerde. Auskunftsrecht und Recht auf korrekte Informationen: Vorbehaltlich des geltenden Rechts hast du das Recht, auf deine Informationen zuzugreifen und sie zu berichtigen. Deine Informationen einsehen und verwalten: Auf deine Informationen zugreifen, Aktivitäten außerhalb von Facebook, Werbepräferenzen, Cookie-Einstellungen, Deine Daten verwalten. Einwilligung widerrufen: Wenn wir uns auf deine Einwilligung zur Verarbeitung deiner Informationen stützen, kannst du deine Einwilligung jederzeit widerrufen. Wenn du deine Einwilligung widerrufst, berührt dies nicht die Rechtmäßigkeit der Verarbeitung, die aufgrund der Einwilligung bis zum Widerruf erfolgte. Um deine Rechte auszuüben, nutze unsere Hilfebereiche, deine Einstellungen für Facebook und Instagram sowie deine gerätebasierten Einstellungen. Deine Informationen übertragen: In bestimmten Fällen und vorbehaltlich des geltenden Rechts hast du das Recht, deine Informationen zu übertragen. Deine Informationen löschen: Wenn rechtsgültige Gründe dafür vorliegen und vorbehaltlich des geltenden Rechts, hast du das Recht zu verlangen, dass wir deine Informationen löschen. Außerdem kannst du Folgendes tun, um deine Informationen zu löschen: Bestimmte Informationen mit Hilfe der zur Verfügung gestellten Kontrollmechanismen zum Löschen finden und löschen Für bestimmte Informationen, die du in unseren Produkten sehen kannst, bieten wir Tools an, die du zum Beantragen einer Löschung nutzen kannst. Beispielsweise kannst du über den Button „Löschen“ Inhalte löschen, die du über dein Konto gepostet hast. Du kannst auch Tools wie Aktivitätenprotokoll auf Facebook nutzen, um Inhalte massenweise in den Papierkorb zu verschieben. Wenn du Inhalte löschst, sind diese nicht länger für andere Nutzer sichtbar. Im Facebook-Hilfebereich bzw. im Instagram-Hilfebereich erfährst du, was geschieht, wenn du deine Inhalte löschst oder in den Papierkorb verschiebst. Dein Konto dauerhaft löschen Wenn du dein Konto auf Facebook oder Instagram löschst, löschen wir deine Informationen, einschließlich der von dir geposteten Dinge, wie beispielsweise deine Fotos und Status-Updates, es sei denn, wir müssen diese Informationen wie im Abschnitt „Wie lange behalten wir deine Informationen?“ beschrieben länger speichern. Hinweis: Sobald dein Konto dauerhaft gelöscht ist, kannst du es nicht wieder reaktivieren, und du kannst von dir hinzugefügte Informationen, einschließlich von dir geposteter Inhalte, nicht mehr abrufen. Wie lange dauert es, deine Informationen zu löschen? Wenn du beantragst, dass wir dein Konto oder deine Inhalte löschen, kann es bis zu 90 Tage dauern, bis die Informationen gelöscht sind, nachdem wir den Kontolöschvorgang starten oder einen Antrag auf Löschung von Inhalten erhalten. Nachdem die Informationen gelöscht wurden, benötigen wir unter Umständen bis zu weitere 90 Tage, um sie aus Sicherungskopien und Notfallwiederherstellungssystemen zu entfernen. Wenn du deine gelöschten Inhalte in deinem Papierkorb auf Facebook oder in deinem „Kürzlich gelöscht“-Ordner auf

Instagram lässt, beginnt der Löschvorgang automatisch nach 30 Tagen. Du kannst den Löschvorgang auch sofort starten, indem du die Inhalte aus deinem Papierkorb oder „Kürzlich gelöscht“-Ordner löschst. Widersprechen: Du hast das Recht, bestimmten Verarbeitungen deiner Informationen zu widersprechen bzw. sie einzuschränken. Abbestellen: Du kannst den „Abbestellen“-Link in unseren Marketingmitteilungen nutzen, damit wir deine Informationen künftig nicht mehr für dieses Direktmarketing verwenden. Widersprechen: Du kannst unserer Verarbeitung deiner Informationen widersprechen, wenn wir uns auf berechnete Interessen stützen oder eine Aufgabe im öffentlichen Interesse erfüllen. Wir werden verschiedene Faktoren berücksichtigen, wenn wir einen Widerspruch bewerten, unter anderem: Die angemessenen Erwartungen unserer Nutzer, Den Nutzen und die Risiken für dich, uns, andere Nutzer oder Dritte, Sonstige verfügbare Mittel zur Erreichung desselben Zwecks, die möglicherweise weniger invasiv sind und keine unverhältnismäßigen Anstrengungen erfordern. Sofern wir nicht feststellen, dass wir zwingende berechnete Gründe für diese Verarbeitung haben, die deine Interessen oder Grundrechte und Grundfreiheiten überwiegen, oder sofern die Verarbeitung nicht aus rechtlichen Gründen erforderlich ist, wird deinem Widerspruch stattgegeben und wir werden die Verarbeitung deiner Informationen einstellen. Weitere Informationen zu den Umständen, unter denen ein Widerspruch erfolgreich sein kann, findest du im Hilfebereich. Eine Beschwerde einreichen: Du kannst außerdem eine Beschwerde bei der für Meta Platforms Ireland Limited zuständigen führenden Aufsichtsbehörde, der irischen Datenschutzkommission, oder bei deiner lokalen Aufsichtsbehörde einreichen. Wie lange behalten wir deine Informationen? Wir behalten deine Informationen so lange, wie wir sie brauchen, um unsere Produkte bereitzustellen, rechtliche Verpflichtungen zu erfüllen oder unsere Interessen oder die Interessen anderer zu schützen. Wir entscheiden von Fall zu Fall, wie lange wir Informationen benötigen. Bei dieser Entscheidung berücksichtigen wir folgende Faktoren: ob wir sie benötigen, um unsere Produkte zu betreiben oder bereitzustellen. Beispielsweise müssen wir einige deiner Informationen aufbewahren, um dein Konto beizubehalten. Für welches Feature wir sie verwenden und wie dieses Feature funktioniert. Beispielsweise werden Nachrichten, die mit dem Selbstlöschmodus von Messenger gesendet werden, weniger lang als normale Nachrichten aufbewahrt. Wie lang wir die Informationen zur Erfüllung bestimmter rechtlicher Verpflichtungen aufbewahren müssen. Ob wir sie für andere berechnete Gründe benötigen, z. B. um Schaden zu verhindern, mögliche Verstöße gegen unsere Nutzungsbedingungen oder Richtlinien zu untersuchen, die Sicherheit und Integrität zu fördern oder uns selbst zu schützen, darunter unsere Rechte, unser Eigentum und unsere Produkte. In einigen Fällen und aus bestimmten Gründen bewahren wir Informationen für einen längeren Zeitraum auf. In unserer Richtlinie erfährst du, wann wir deine Informationen aufbewahren dürfen. Wenn wir sie benötigen, um unsere Produkte zu betreiben oder bereitzustellen: Zum Beispiel bewahren wir Profilinformationen, Fotos, die du gepostet (und nicht gelöscht) hast, und Sicherheitsinformationen auf, solange dein Konto besteht. Und wenn du auf Facebook nach etwas suchst, bewahren wir den Suchverlauf so lange auf, bis du die Suchanfragen in deinem Aktivitätenprotokoll entfernst oder dein Konto löschst. Sobald du eine Suchanfrage entfernst oder dein Konto löschst, ist diese bzw. dieses nicht mehr für dich sichtbar und wird gelöscht. Doch selbst wenn du deine Suchanfrage nicht entfernst oder dein Konto nicht löschst, löschen wir sechs Monate nach deiner Suche Informationen zu dieser Suchanfrage, die nicht notwendig sind, um dir deinen Suchverlauf anzuzeigen. Dies sind Informationen zu dem von dir verwendeten Gerät oder deinem Standort. Für welches Feature wir sie verwenden und wie dieses Feature funktioniert. Beispiel: May plant eine Überraschungsparty für Yang. In Messenger sendet sie Cynthia die Details zur Party mit dem Selbstlöschmodus, sodass die Nachricht verschwindet. Die Nachricht wird May nicht mehr angezeigt, sobald sie den Chat verlässt, und Cynthia sieht die Nachricht nur das erste Mal, wenn sie den Nachrichtenverlauf öffnet. Nachdem Cynthia die Nachricht gelesen hat, wird der Inhalt nach einer Stunde gelöscht. Wenn Cynthia die Nachricht nicht liest, wird sie nach 14 Tagen gelöscht. Wie lange wir die Informationen zur Erfüllung bestimmter rechtlicher Verpflichtungen aufbewahren müssen: Wir bewahren Informationen beispielsweise so lange auf, wie wir sie für Folgendes benötigen: Eine rechtliche Anfrage oder Verpflichtung, einschließlich Verpflichtungen von Meta-Unternehmen, oder zur Einhaltung des anwendbaren Rechts, Eine behördliche Untersuchung, Einen rechtlichen Anspruch, eine Beschwerde, eine Rechtsstreitigkeit oder ein regulatorisches Verfahren. Aus diesen Gründen können wir deine Informationen länger aufbewahren: Deine Informationen, einschließlich Daten zu finanziellen Transaktionen, die mit auf unseren Produkten getätigten Käufen oder Geldtransfers zusammenhängen, können länger aufbewahrt werden bzw. der Zugriff darauf kann länger erfolgen, wenn sie sich auf Folgendes beziehen: Eine rechtliche Anfrage oder Verpflichtung, einschließlich Verpflichtungen von Meta-Unternehmen, oder zur Einhaltung des anwendbaren Rechts: Eine behördliche Untersuchung, Eine Untersuchung auf mögliche Verstöße gegen unsere Nutzungsbedingungen oder Richtlinien, Zur Schadenvermeidung, Zu Zwecken von Schutz, Sicherheit und Integrität, Zu unserem Schutz, einschließlich unserer Rechte, unseres Eigentums, unserer Mitarbeiter oder Produkte, Wenn die Informationen in Zusammenhang mit einem rechtlichen

Anspruch, einer Rechtsstreitigkeit oder einem regulatorischen Verfahren stehen. In einigen Fällen können wir deine Informationen aus den oben genannten Gründen auch dann aufbewahren, wenn du die Löschung deines Kontos oder einiger deiner Inhalte beantragt hast. Möglicherweise bewahren wir außerdem Informationen von Konten, die deaktiviert wurden, und Inhalte auf, die aufgrund von Verstößen gegen unsere Nutzungsbedingungen und Richtlinien verstoßen. Deine Informationen oder dein Konto löschen: Du kannst Folgendes tun, um deine Informationen zu löschen: Bestimmte Informationen suchen und löschen Wir haben Tools, die du nutzen kannst, um bestimmte Informationen zu löschen. Beispielsweise kannst du über den Button „Löschen“ Inhalte löschen, die du über dein Konto gepostet hast. Du kannst auch Tools wie Aktivitätenprotokoll auf Facebook nutzen, um Inhalte massenweise in den Papierkorb zu verschieben. Wenn du Inhalte löschst, sind diese nicht länger für andere Nutzer sichtbar. Im Facebook-Hilfebereich bzw. im Instagram-Hilfebereich erfährst du, was geschieht, wenn du deine Inhalte löschst oder in den Papierkorb verschiebst. Dein Konto dauerhaft löschen. Wenn du dein Konto auf Facebook oder Instagram löschst, löschen wir deine Informationen, einschließlich der von dir geposteten Dinge, wie beispielsweise deine Fotos und Status-Updates, es sei denn, wir müssen sie wie im Abschnitt „Wie lange behalten wir deine Informationen?“ beschrieben länger speichern. Sobald dein Konto dauerhaft gelöscht ist, kannst du es nicht wieder reaktivieren, und du kannst Informationen, einschließlich von dir geposteter Inhalte, nicht mehr abrufen. Wie lange dauert es, deine Informationen zu löschen? Wenn du beantragst, dass wir dein Konto oder deine Inhalte löschen, kann es bis zu 90 Tage dauern, bis die Informationen gelöscht sind, nachdem wir den Kontolöschvorgang starten oder einen Antrag auf Löschung von Inhalten erhalten. Nachdem die Informationen gelöscht wurden, benötigen wir unter Umständen bis zu weitere 90 Tage, um sie aus Sicherungskopien und Notfallwiederherstellungssystemen zu entfernen. Wenn du deine gelöschten Inhalte in deinem Papierkorb auf Facebook oder in deinem „Kürzlich gelöscht“-Ordner auf Instagram lässt, beginnt der Löschvorgang automatisch nach 30 Tagen. Du kannst den Löschvorgang auch sofort starten, indem du die Inhalte aus deinem Papierkorb oder „Kürzlich gelöscht“-Ordner löschst. Beispiele, warum wir deine Informationen unter Umständen aufbewahren: Als Reaktion auf eine rechtliche Anfrage: Wir bewahren deine Informationen möglicherweise nach der Löschung deines Kontos auf, wenn wir eine wirksame rechtliche Anordnung erhalten, wie zum Beispiel eine Aufbewahrungsanordnung oder einen Durchsuchungsbeschluss, die in Zusammenhang mit deinem Konto stehen. Um geltende Gesetze einzuhalten: Beispielsweise bewahren wir gemäß Metas Buchhaltungspflichten bestimmte Informationen zu Käufen oder Transaktionen auf, die mit einem Konto verknüpft sind. Zu Zwecken von Schutz, Sicherheit und Integrität: Wenn wir zum Beispiel ein Konto aufgrund von Verstößen gegen unsere Nutzungsbedingungen oder Richtlinien deaktivieren, bewahren wir Informationen über diesen Nutzer auf, um ihn daran zu hindern, ein neues Konto zu erstellen. Unter Umständen bewahren wir außerdem einige deiner Kontoinformationen im Rahmen unserer Überprüfung auf verdächtige Aktivitäten auf. Dazu gehören jegliche verdächtige Aktivitäten in Verbindung mit unseren finanziellen Produkten, wie zum Beispiel Geldwäsche oder die Finanzierung von Terroristen. Für Rechtsstreitigkeiten: Wir bewahren deine Informationen möglicherweise auf, wenn wir es aufgrund eines rechtlichen Anspruchs oder einer Beschwerde für notwendig halten. Beispielsweise müssen wir uns unter Umständen in einem Rechtsverfahren gegen eine Klage im Zusammenhang mit deinen Daten verteidigen. Wie übermitteln wir Informationen? Warum werden Informationen in andere Länder übermittelt? Wir teilen die von uns erhobenen Informationen weltweit, sowohl intern zwischen unseren Niederlassungen und Rechenzentren als auch extern mit unseren Partnern, Anbietern, Dienstleistern und Dritten. Da Meta global tätig ist und Nutzer, Partner sowie Mitarbeiter auf der ganzen Welt hat, sind Übermittlungen aus vielerlei Gründen notwendig, wie u. a.: Damit wir die in den Nutzungsbedingungen für das von dir genutzte Meta-Produkt und in dieser Richtlinie genannten Dienste betreiben und bereitstellen können. Hierzu gehört auch, es dir zu ermöglichen, weltweit Informationen zu teilen und dich mit deiner Familie und deinen Freunden zu vernetzen. Damit wir unsere Produkte reparieren, analysieren und verbessern können. Wohin werden Informationen übermittelt? Von Meta Platforms Ireland Limited kontrollierte Informationen werden in folgende Länder übertragen oder übermittelt oder dort gespeichert und verarbeitet: Orte, an denen wir Infrastruktur oder Rechenzentren haben, wie u. a. die USA, Irland, Dänemark und Schweden, Länder, in denen Produkte der Meta-Unternehmen verfügbar sind, Andere Länder außerhalb des Landes, in dem du lebst, in denen unsere Partner, Anbieter, Dienstleister und Dritten ansässig sind, für die in dieser Richtlinie beschriebenen Zwecke. Wie schützen wir deine Informationen? Wir stützen uns auf angemessene Mechanismen für internationale Datenübermittlungen. Außerdem stellen wir sicher, dass bei jeder Übermittlung deiner Informationen angemessene Schutzmaßnahmen vorhanden sind. Beispielsweise verschlüsseln wir deine Informationen während der Übermittlung über öffentliche Netzwerke, um sie vor unberechtigtem Zugriff zu schützen. Mechanismen, die wir für die globale Datenübermittlung nutzen: Wir stützen uns auf angemessene Mechanismen für internationale Datenübermittlungen. Beispiel: Für Informationen, die wir erheben: verlassen wir uns auf die Beschlüsse der Europäischen Kommission, gemäß denen sie anerkennen, dass bestimmte Länder

und Gebiete außerhalb des Europäischen Wirtschaftsraums ein angemessenes Datenschutzniveau für personenbezogene Daten gewährleisten. Diese Beschlüsse werden als „Angemessenheitsbeschlüsse“ bezeichnet. Übermitteln wir die von uns erhobenen Informationen aus dem Europäischen Wirtschaftsraum nach Argentinien, Israel, Neuseeland und in die Schweiz und, sofern die Entscheidung anwendbar ist, nach Kanada und verlassen uns dabei auf einen Angemessenheitsbeschluss. Erfahre mehr zu Angemessenheitsbeschlüssen für die jeweiligen Länder. In anderen Fällen verlassen wir uns bei der Datenübermittlung in ein Drittland auf Standardvertragsklauseln, die von der Europäischen Kommission genehmigt wurden (und auf die entsprechenden Standardvertragsklauseln des Vereinigten Königreichs, sofern anwendbar), oder auf Ausnahmen, die nach anwendbarem Recht vorgesehen sind. Beispielweise liegt derzeit kein Angemessenheitsbeschluss für die USA vor, daher verlassen wir uns bei der Datenübermittlung an Meta Platforms, Inc. auf Standardvertragsklauseln. Zusätzlich zu den Standardvertragsklauseln ergreifen wir auch ergänzende Maßnahmen, um einen entsprechenden Schutz bei der Übermittlung deiner Daten gewährleisten zu können. Wenn du Fragen zu den internationalen Datenübermittlungen und den Standardvertragsklauseln von Meta hast, kannst du uns kontaktieren.

Angemessenheitsbeschlüsse: Erfahre mehr zu Angemessenheitsbeschlüssen für die jeweiligen Länder: Argentinien, Kanada, Israel, Neuseeland, Schweiz. Wie reagieren wir auf rechtliche Anfragen, wie halten wir geltendes Recht ein bzw. wie verhindern wir Schäden? Aus folgenden Gründen greifen wir auf deine Informationen zu und speichern, verwenden und teilen sie: als Reaktion auf rechtliche Anfragen wie Durchsuchungsbeschlüsse, gerichtliche Entscheidungen, gerichtliche Aufträge zur Herausgabe von Kundeninformationen oder Vorladungen. Diese Anfragen stammen von Dritten wie zum Beispiel von Prozessführenden in Zivilprozessen oder von Strafverfolgungs- und anderen Behörden. Mehr dazu, wie wir auf rechtliche Anfragen reagieren. Im Einklang mit geltendem Recht, um den Schutz, die Sicherheit und die Integrität von Meta-Produkten, der Nutzer, der Mitarbeiter, des Eigentums und der Öffentlichkeit sicherzustellen. Möglicherweise können wir für einen längeren Zeitraum auf deine Informationen zugreifen oder sie speichern. So begegnen wir rechtlichen Fragen: Wir begegnen rechtlichen Fragen, wenn wir in gutem Glauben davon ausgehen, dass wir gesetzlich dazu verpflichtet sind. Wir können auch auf bestimmte rechtliche Anfragen reagieren, wenn wir zwar nicht gesetzlich dazu verpflichtet sind, jedoch in gutem Glauben davon ausgehen, dass eine Reaktion: in der jeweiligen Rechtsordnung gesetzlich vorgeschrieben ist, Nutzer in dieser Rechtsordnung beeinträchtigt, und sich mit international anerkannten Standards deckt, einschließlich unserer unternehmensweiten Menschenrechtsrichtlinie. Erfahre mehr zu Regierungsanfragen und wie wir reagiert haben. So fördern wir Schutz, Integrität und Sicherheit: Wir geben wir deine Informationen an Strafverfolgungsbehörden, Regierungsbehörden, Meta-Unternehmen, Dritte (einschließlich Branchenkollegen) und andere weiter, wenn wir in gutem Glauben davon ausgehen, dass dies notwendig ist, um eine Vielzahl von Situationen zu erkennen, zu verhindern und zu verfolgen, darunter: die unberechtigte Nutzung unserer Produkte. Ein Beispiel ansehen, Verstöße gegen unsere Nutzungsbedingungen und Richtlinien, Verdächtige Aktivitäten untersuchen, Uns selbst schützen, einschließlich unserer Rechte, unseres Eigentums, unserer Mitarbeiter oder Produkte, Missbrauch, Betrug und andere schädliche oder illegale Aktivitäten in und außerhalb unserer Produkte verhindern, Dich und andere schützen, einschließlich im Rahmen einer Untersuchung oder behördlichen Anfrage, Notfallsituationen, wie zum Beispiel Lebensgefahr oder das Risiko einer drohenden Körperverletzung. Aus diesen Gründen können wir deine Informationen länger aufbewahren: Deine Informationen, einschließlich Daten zu finanziellen Transaktionen, die mit auf unseren Produkten getätigten Käufen oder Geldtransfers zusammenhängen, können länger aufbewahrt werden bzw. der Zugriff darauf kann länger erfolgen, wenn sie sich auf Folgendes beziehen: Eine rechtliche Anfrage oder Verpflichtung, einschließlich Verpflichtungen von Meta-Unternehmen, oder zur Einhaltung des anwendbaren Rechts, Eine behördliche Untersuchung, Eine Untersuchung auf mögliche Verstöße gegen unsere Nutzungsbedingungen oder Richtlinien, Zur Schadensvermeidung, Zu Zwecken von Schutz, Sicherheit und Integrität, Zu unserem Schutz, einschließlich unserer Rechte, unseres Eigentums, unserer Mitarbeiter oder Produkte, Wenn die Informationen in Zusammenhang mit einem rechtlichen Anspruch, einer Rechtsstreitigkeit oder einem regulatorischen Verfahren stehen. In einigen Fällen können wir deine Informationen aus den oben genannten Gründen auch dann aufbewahren, wenn du die Löschung deines Kontos oder einiger deiner Inhalte beantragt hast. Möglicherweise bewahren wir außerdem Informationen von Konten, die deaktiviert wurden, und Inhalte auf, die aufgrund von Verstößen gegen unsere Nutzungsbedingungen und Richtlinien verstoßen. Unberechtigte Nutzung unserer Produkte: Wenn du beispielsweise unrechtmäßig Daten von Facebook-Nutzern erhebst und nutzt, können wir deine Informationen weitergeben, um uns selbst gegen Klagen oder in Rechtsstreitigkeiten zu verteidigen. Verstöße gegen unsere Nutzungsbedingungen und Richtlinien: Wenn du zum Beispiel drohende oder gefährliche Inhalte veröffentlichst, können wir deine Informationen über die Meta-Unternehmen hinweg weitergeben, um uns selbst und andere zu schützen. Dies kann das Blockieren deines Zugriffs auf bestimmte Funktionen oder das Deaktivieren

deines Kontos über die Meta-Unternehmen hinweg umfassen. Beispiele, warum wir deine Informationen unter Umständen aufbewahren: Als Reaktion auf eine rechtliche Anfrage: Wir bewahren deine Informationen möglicherweise nach der Löschung deines Kontos auf, wenn wir eine wirksame rechtliche Anordnung erhalten, wie zum Beispiel eine Aufbewahrungsanordnung oder einen Durchsuchungsbeschluss, die in Zusammenhang mit deinem Konto stehen. Um geltende Gesetze einzuhalten: Beispielsweise bewahren wir gemäß Metas Buchhaltungspflichten bestimmte Informationen zu Käufen oder Transaktionen auf, die mit einem Konto verknüpft sind. Zu Zwecken von Schutz, Sicherheit und Integrität: Wenn wir zum Beispiel ein Konto aufgrund von Verstößen gegen unsere Nutzungsbedingungen oder Richtlinien deaktivieren, bewahren wir Informationen über diesen Nutzer auf, um ihn daran zu hindern, ein neues Konto zu erstellen. Unter Umständen bewahren wir außerdem einige deiner Kontoinformationen im Rahmen unserer Überprüfung auf verdächtige Aktivitäten auf. Dazu gehören jegliche verdächtige Aktivitäten in Verbindung mit unseren finanziellen Produkten, wie zum Beispiel Geldwäsche oder die Finanzierung von Terroristen. Für Rechtsstreitigkeiten: Wir bewahren deine Informationen möglicherweise auf, wenn wir es aufgrund eines rechtlichen Anspruchs oder einer Beschwerde für notwendig halten. Beispielsweise müssen wir uns unter Umständen in einem Rechtsverfahren gegen eine Klage im Zusammenhang mit deinen Daten verteidigen. Wie erfährst du, dass sich die Richtlinie geändert hat? Wir benachrichtigen dich, bevor wir wesentliche Änderungen an dieser Richtlinie vornehmen. Du erhältst dann die Gelegenheit, die überarbeitete Richtlinie zu überprüfen, bevor du dich dazu entscheidest, unsere Produkte weiterhin zu nutzen. So kontaktierst du Meta bei Fragen: Weitere Informationen zur Funktionsweise des Datenschutzes findest du auf Facebook, auf Instagram und im Facebook-Hilfebereich. Bei Fragen zu dieser Richtlinie oder bei Fragen, Beschwerden oder Anfragen bezüglich deiner Informationen kannst du uns wie unten beschrieben kontaktieren. Der Datenverantwortliche bezüglich deiner Informationen ist Meta Platforms Ireland Limited. Dieses Unternehmen kannst du online kontaktieren oder per Post unter: Meta Platforms Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Irland. Kontaktaufnahme mit dem Datenschutzbeauftragten für Meta Platforms Ireland Limited. Du hast außerdem das Recht, eine Beschwerde bei der für Facebook Ireland zuständigen führenden Aufsichtsbehörde, der irischen Datenschutzkommission, oder bei deiner lokalen Aufsichtsbehörde einzureichen. Informationen zur Rechtsgrundlage: Einwilligung: Wir verarbeiten Informationen wie im Folgenden beschrieben, wenn du uns deine Einwilligung dazu erteilt hast. Diese Einwilligung können wir über produktinterne Erlebnisse, zur Aktivierung bestimmter Funktionen oder zur Aktivierung gerätebasierter Einstellungen einholen. Welche Informationskategorien wir nutzen sowie warum und wie sie verarbeitet werden, wird nachstehend erläutert: Verarbeitung von Informationen mit besonderem Schutz, die du uns zur Verfügung stellst, damit wir sie mit den von dir ausgewählten Personen teilen, unsere Produkte bereitstellen, personalisieren und verbessern sowie Analysen durchführen können. Zu diesen Zwecken erheben, speichern, veröffentlichen und nutzen wir automatisierte oder manchmal auch manuelle Verarbeitungen. Deine Aktivität und die von dir bereitgestellten Informationen: Informationen mit besonderem Schutz, die du freiwillig in deinen Profildern (wie zum Beispiel deine religiösen Ansichten, politische Einstellung oder für wen du dich „interessierst“) oder im Rahmen von Umfragen angibst, an denen du freiwillig teilnimmst, und dort, wo du deine ausdrückliche Einwilligung erteilt hast. Nutzung von Informationen Dritter, um die Werbung, die dir angezeigt wird, auf dich zuzuschneiden: Wir verwenden Informationen, die Partner uns bezüglich Aktivitäten außerhalb der Meta-Produkte bereitstellen und die wir mit dir verknüpft haben, um Werbeanzeigen zu personalisieren, die wir dir auf den Meta-Produkten sowie auf Websites, Apps und Geräten, die unsere Werbedienste nutzen, zeigen. Wir erhalten diese Informationen unabhängig davon, ob du bei unseren Produkten angemeldet bist bzw. ein Konto auf ihnen hast oder nicht. Mehr dazu erfährst du in der Cookie-Richtlinie. Informationen von Partnern, Anbietern und Dritten. Weitergabe deiner Kontakt-, Profil- oder sonstiger Informationen an Dritte auf Antrag von dir: Um welche Art von Dritten es sich handelt und welche Kategorien von Informationen wir weitergeben, hängt davon ab, unter welchen Umständen du uns bittest, etwas weiterzugeben. Zum Beispiel teilen wir deine E-Mail-Adresse (oder sonstige Kontaktinformationen) oder andere Informationen, die du gegebenenfalls beschließt, freiwillig zu teilen, wenn du uns anweist, sie an einen Werbetreibenden weiterzugeben, damit dieser dich mit zusätzlichen Informationen über ein beworbenes Produkt kontaktieren kann. Deine Aktivität und die von dir bereitgestellten Informationen: Inhalte, die du erstellst, wie deine Kontakt-, Profil- oder sonstige Informationen wie Beiträge oder Kommentare. Erheben von Informationen, deren Erhalt du uns durch die von dir aktivierten gerätebasierten Einstellungen gestattest (wie den Zugriff auf deinen GPS-Standort, deine Kamera oder Fotos), damit wir diese nutzen können, um die bei der Aktivierung der Einstellung beschriebenen Funktionen oder Dienste bereitzustellen. App-, Browser- und Geräteinformationen: Informationen aus den Geräteeinstellungen. Wenn wir Informationen verarbeiten, die du uns auf Grundlage deiner Einwilligung bereitgestellt hast, hast du das Recht, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund deiner Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt

wird. Du hast auch das Recht, die Informationen, die du uns auf der Grundlage deiner Einwilligung zur Verfügung stellst, zu übertragen. Um deine Rechte auszuüben, nutze deine gerätebasierten Einstellungen sowie die Facebook-Einstellungen, die Instagram-Einstellungen und unsere Hilfebereiche. Erfüllung eines Vertrags: In Bezug auf alle Personen, die die Geschäftsfähigkeit zum Abschluss eines durchsetzbaren Vertrags haben (z. B. weil sie im Land ihres Wohnsitzes volljährig sind), verarbeiten wir die Informationen in dem für den Abschluss und die Erfüllung unserer Verträge mit dir erforderlichen Maß (die Meta-Nutzungsbedingungen und Instagram-Nutzungsbedingungen, die Ergänzenden Nutzungsbedingungen von Meta Platforms Technologies, die Ergänzenden Portal-Nutzungsbedingungen und die Ergänzenden Meta View-Nutzungsbedingungen, zusammen „die Nutzungsbedingungen“). Die Zwecke, für die wir Informationen zur Erfüllung unserer Verträge verarbeiten, die von uns verwendeten Informationskategorien und wie die Informationen verarbeitet werden, wird nachstehend erläutert: Personalisierung der Meta-Produkte: Unsere Systeme verarbeiten automatisch Informationen, die wir im Zusammenhang mit dir und anderen Personen erhoben und gespeichert haben, um deine Interessen und Präferenzen zu bewerten und zu verstehen und dir über die Meta-Produkte hinweg gemäß unseren Nutzungsbedingungen personalisierte Erlebnisse zu bieten. Auf diese Weise: personalisieren wir Funktionen und Inhalte (wie deinen News Feed, Instagram-Feed und Stories); personalisieren wir die Werbeanzeigen, die den Nutzern angezeigt werden, und können wir dir auf unseren Produkten bzw. außerhalb dieser Vorschläge unterbreiten (z. B. Personen, die du kennen könntest, Gruppen oder Veranstaltungen, für die du dich interessieren könntest, oder Themen, die du eventuell abonnieren möchtest). Erfahre mehr dazu, wie wir Informationen über dich verwenden, um dein Erlebnis in und auf den Meta-Produkten zu personalisieren, und wie wir die Werbeanzeigen auswählen, die dir angezeigt werden. Deine Aktivität und die von dir bereitgestellten Informationen: Inhalte, die du erstellst, wie Beiträge oder Kommentare oder Audio, Inhalte, die du über unsere Kamerafunktion oder deine Einstellungen für Aufnahmen oder über unsere sprachgestützten Funktionen bereitstellst, Metadaten zu Inhalten, Die Arten von Inhalten, die du dir ansiehst bzw. mit denen du interagierst, Die Apps und Funktionen, die du nutzt, und welche Handlungen du in ihnen durchführst, Käufe oder andere Transaktionen, die du ausführst, Hashtags, die du verwendest, Den Zeitpunkt, die Häufigkeit und die Dauer deiner Aktivitäten auf unseren Produkten, Freunde, Follower und andere Kontakte, App-, Browser- und Geräteinformationen: Geräteeigenschaften und Gerätesoftware, Was du gerade auf deinem Gerät tust (z. B. ob sich unsere App im Vordergrund befindet oder ob sich deine Maus bewegt), Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, Gerätesignale, Informationen, die du über deine Geräteeinstellungen geteilt hast (wie GPS-Standort), Informationen zum Netzwerk, mit dem du dein Gerät verbindest, Berichte über die Performance unserer Produkte auf deinem Gerät, Informationen von Cookies und ähnlichen Technologien. Informationen von Partnern, Anbietern und Dritten (außer Verwendung von Partnerdaten, um Werbung auf dich zuzuschneiden). Bereitstellung und Verbesserung unserer Meta-Produkte: Die Bereitstellung der Meta-Produkte umfasst die Erhebung, das Speichern und ggf. Teilen, Profiling, Überprüfen und Kuratieren und in einigen Fällen nicht nur die automatisierte Verarbeitung, sondern auch das manuelle (menschliche) Überprüfen, um: dein Konto und Profil zu erstellen und zu verwalten, das Teilen von Inhalten und Status zu ermöglichen, Funktionen bereitzustellen und zu kuratieren, Messaging-Dienste bereitzustellen sowie die Möglichkeit, Sprach- und Videoanrufe zu tätigen und sich mit anderen zu verbinden, Werbeprodukte bereitzustellen und Analysen durchzuführen. Wir verwenden Informationen, die uns vorliegen, auch, um Verbesserungen an unseren Produkten zu entwickeln, zu erforschen und zu testen. Wir verwenden die von uns erhobenen Informationen zu folgenden Zwecken: Sehen, ob ein Produkt ordnungsgemäß funktioniert, Nach Fehlern suchen und diese gegebenenfalls beheben, Neue Produkte und Funktionen testen, um deren Funktionalität zu prüfen, Feedback zu unseren Ideen für Produkte oder Funktionen einholen, Durchführung von Umfragen und anderen Studien dazu, was dir an unseren Produkten und Marken gefällt und was wir noch besser machen können. Deine Aktivität und die von dir bereitgestellten Informationen: Inhalte, die du erstellst, wie Beiträge oder Kommentare oder Audio, Inhalte, die du über unsere Kamerafunktion oder deine Einstellungen für Aufnahmen oder über unsere sprachgestützten Funktionen bereitstellst, Nachrichten, die du sendest und empfangst, einschließlich ihrer Inhalte, vorbehaltlich des anwendbaren Rechts, Metadaten zu Inhalten und Nachrichten, Die Arten von Inhalten, die du dir ansiehst bzw. mit denen du interagierst, Die Apps und Funktionen, die du nutzt, und welche Handlungen du in ihnen durchführst, Käufe, die du tätigt, oder andere Transaktionen, die du durchführst, einschließlich gekürzter Kreditkartendaten, Hashtags, die du verwendest, Den Zeitpunkt, die Häufigkeit und die Dauer deiner Aktivitäten auf unseren Produkten, Freunde, Follower und andere Kontakte, App-, Browser- und Geräteinformationen: Geräteeigenschaften und Gerätesoftware, Was du gerade auf deinem Gerät tust (z. B. ob sich unsere App im Vordergrund befindet oder ob sich deine Maus bewegt), Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, Gerätesignale, Informationen, die du über deine Geräteeinstellungen geteilt hast, Informationen zum Netzwerk, mit dem du dein Gerät verbindest,

einschließlich deiner IP-Adresse, Informationen von Cookies und ähnlichen Technologien, Informationen von Partnern, Anbietern und Dritten. Förderung von Schutz, Integrität und Sicherheit in und auf den Meta-Produkten: Die Meta-Produkte sollen dazu beitragen, den Schutz, die Integrität und die Sicherheit dieser Dienste und der Menschen, die sie nutzen, sicherzustellen. Wir verarbeiten Informationen, die wir mit dir verknüpft haben, und wenden dabei automatisierte Verarbeitungstechniken an und führen in einigen Fällen eine manuelle (menschliche) Überprüfung durch, um: Konten und Aktivitäten zu verifizieren, Verstöße gegen unsere Nutzungsbedingungen oder Richtlinien zu ermitteln und zu verfolgen. In einigen Fällen werden die von uns zu Verstößen getroffenen Entscheidungen vom Oversight Board überprüft, um verdächtige Aktivitäten zu untersuchen, schädliches oder rechtswidriges Verhalten zu erkennen, zu verhindern und zu bekämpfen, z. B. durch Überprüfen und in einigen Fällen Entfernen von Inhalten, die uns gemeldet wurden, Spam und andere negative Erlebnisse aufzudecken und zu verhindern, Bedrohungen unseres Personals bzw. Eigentums aufzudecken und zu unterbinden, und die Integrität unserer Produkte zu wahren. Um weitere Informationen zu Schutz, Integrität und Sicherheit im Allgemeinen im Zusammenhang mit Meta-Produkten zu erhalten, besuche den Facebook-Sicherheitsbereich und die Instagram-Sicherheitstipps. Deine Aktivität und die von dir bereitgestellten Informationen: Inhalte, die du erstellst, wie Beiträge oder Kommentare oder Audio, Inhalte, die du über unsere Kamerafunktion oder deine Einstellungen für Aufnahmen oder über unsere sprachgestützten Funktionen bereitstellst, Metadaten zu Inhalten und Nachrichten, Die Arten von Inhalten, die du dir ansiehst bzw. mit denen du interagierst, Die Apps und Funktionen, die du nutzt, und welche Handlungen du in ihnen durchführst, Käufe, die du tätigt, oder andere Transaktionen, die du durchführst, einschließlich gekürzter Kreditkartendaten, Hashtags, die du verwendest, Den Zeitpunkt, die Häufigkeit und die Dauer deiner Aktivitäten auf unseren Produkten, Freunde, Follower und andere Kontakte App-, Browser- und Geräteinformationen: Geräteeigenschaften und Gerätesoftware, Was du gerade auf deinem Gerät tust (z. B. ob sich unsere App im Vordergrund befindet oder ob sich deine Maus bewegt), Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, Gerätesignale, Informationen, die du über deine Geräteeinstellungen geteilt hast, Informationen zum Netzwerk, mit dem du dein Gerät verbindest, einschließlich deiner IP-Adresse, Informationen von Cookies und ähnlichen Technologien, Informationen von Partnern, Anbietern und Dritten. Für die Kommunikation mit dir: Wir verwenden die Informationen, die du uns zur Verfügung gestellt hast (wie Kontaktinformationen in deinem Profil), um dir eine Mitteilung zu senden, wie eine E-Mail oder einen Hinweis in einem Produkt, zum Beispiel in folgenden Fällen: Wir kontaktieren dich per E-Mail oder per Benachrichtigung innerhalb der Produkte im Zusammenhang mit den Meta-Produkten, produktbezogenen Angelegenheiten, Forschung oder um dich über unsere Nutzungsbedingungen und Richtlinien zu informieren. Wir verwenden auch Kontaktinformationen wie deine E-Mail-Adresse, um zu antworten, wenn du uns kontaktierst. Deine Aktivität und die von dir bereitgestellten Informationen: Kontaktinformationen in deinem Profil und deine Kommunikation mit uns, Inhalte, die du erstellst, wie Beiträge oder Kommentare oder Audio, Inhalte, die du über unsere Kamerafunktion oder deine Einstellungen für Aufnahmen oder über unsere sprachgestützten Funktionen bereitstellst. App-, Browser- und Geräteinformationen: Geräteeigenschaften und Gerätesoftware, Was du gerade auf deinem Gerät tust (z. B. ob sich unsere App im Vordergrund befindet oder ob sich deine Maus bewegt), Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, Gerätesignale, Informationen, die du über deine Geräteeinstellungen geteilt hast, Informationen zum Netzwerk, mit dem du dein Gerät verbindest, einschließlich deiner IP-Adresse, Informationen von Cookies und ähnlichen Technologien. Übermittlung, Speicherung oder Verarbeitung deiner Informationen in Ländern außerhalb des EWR, einschließlich in den USA und anderen Ländern: Wir teilen von uns erhobene Informationen weltweit, sowohl intern zwischen unseren Niederlassungen und Rechenzentren als auch extern mit unseren Partnern, Dritten und Dienstleistern. Da Meta global tätig ist und Nutzer, Partner sowie Mitarbeiter auf der ganzen Welt hat, sind Übermittlungen für folgende Zwecke notwendig: um die Dienste zu betreiben und bereitzustellen, die in den Nutzungsbedingungen beschrieben werden, die für das/die von dir genutzte(n) Meta-Produkt(e) gelten. Hierzu gehört auch, es dir zu ermöglichen, weltweit Informationen zu teilen und dich mit deiner Familie und deinen Freunden zu vernetzen; und damit wir unsere Produkte reparieren, analysieren und verbessern können. Deine Aktivität und die von dir bereitgestellten Informationen: Inhalte, die du erstellst, wie Beiträge oder Kommentare oder Audio, Inhalte, die du über unsere Kamerafunktion oder deine Einstellungen für Aufnahmen oder über unsere sprachgestützten Funktionen bereitstellst, Metadaten zu Inhalten und Nachrichten, Die Arten von Inhalten, die du dir ansiehst bzw. mit denen du interagierst, Die Apps und Funktionen, die du nutzt, und welche Handlungen du in ihnen durchführst, Käufe, die du tätigt, oder andere Transaktionen, die du durchführst, einschließlich gekürzter Kreditkartendaten, Hashtags, die du verwendest, Den Zeitpunkt, die Häufigkeit und die Dauer deiner Aktivitäten auf unseren Produkten, Freunde, Follower und andere Kontakte, App-, Browser- und Geräteinformationen: Geräteeigenschaften und Gerätesoftware, Was du gerade auf deinem Gerät tust

(z. B. ob sich unsere App im Vordergrund befindet oder ob sich deine Maus bewegt), Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, Gerätesignale, Informationen, die du über deine Geräteeinstellungen geteilt hast, Informationen zum Netzwerk, mit dem du dein Gerät verbindest, einschließlich deiner IP-Adresse, Informationen von Cookies und ähnlichen Technologien, Informationen von Partnern, Anbietern und Dritten. Wir verwenden die uns zur Verfügung stehenden Informationen, um diese Dienste bereitzustellen. Wenn du dich gegen die Bereitstellung bestimmter Informationen entscheidest (abgesehen von einigen Kontoinformationen, die erforderlich sind, um ein Facebook-Konto oder ein Instagram-Konto zu erstellen), kann dein Erlebnis bei der Nutzung der Meta-Produkte beeinträchtigt werden. Zum Beispiel siehst du möglicherweise weniger relevante Empfehlungen in den Produkten oder deine Nutzung der Produkte kann eingeschränkt sein. Wenn wir Informationen verarbeiten, die du uns als für den Abschluss und die Erfüllung unserer Verträge mit dir erforderlich bereitstellst, hast du gemäß der DSGVO das Recht auf Datenübertragbarkeit. Um deine Rechte auszuüben, gehe bitte zu den Facebook-Einstellungen, den Instagram-Einstellungen oder informiere dich in unseren Hilfebereichen. Erfüllung einer rechtlichen Verpflichtung: Welche Informationskategorien wir verwenden, warum wir deine Informationen Daten aufgrund der Erfüllung einer rechtlichen Verpflichtung verarbeiten und wie die Verarbeitung erfolgt, ist nachstehend dargelegt: Für die Verarbeitung von Informationen, wenn dies nach dem Gesetz erforderlich ist: Wenn wir zur Offenlegung von Informationen verpflichtet sind, beispielsweise wenn es eine gültige rechtliche Anfrage für bestimmte Informationen gibt (etwa einen irischen Durchsuchungsbeschluss) werden wir auf deine Informationen zugreifen, sie aufbewahren und/oder sie an Aufsichtsbehörden, Strafverfolgungs- oder andere Behörden weitergeben. Die Art und Weise, wie die Informationen verarbeitet werden, hängt von den jeweiligen Umständen ab. Mehr dazu erfährst du unter Wie antworten wir auf rechtliche Anfragen, verhindern Schäden und fördern die Sicherheit und Integrität? Unter Informationen für Strafverfolgungsbehörden geben wir Informationen zu den operativen Richtlinien, die die Strafverfolgungsbehörden befolgen müssen. Beispiele für irische Gesetze und in Irland durchsetzbare EU-Gesetze, durch die eine Verpflichtung entstehen könnte, sodass wir zur Verarbeitung der Informationen, die wir über dich gespeichert haben, verpflichtet sind: Zivil- und Handelssachen: wenn wir eine gerichtliche Entscheidung erhalten oder anderweitig verpflichtet sind, Informationen für die Zwecke von Gerichtsverfahren offenzulegen, z. B. im Rahmen der Verordnung (EU) Nr. 1215/2012 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen. Strafsachen: zur Erfüllung von Anfragen von irischen Strafverfolgungsbehörden zur Bereitstellung von Informationen im Zusammenhang mit einer Untersuchung, z. B. im Rahmen von Section 10 des Criminal Justice (Miscellaneous Provisions) Act 1997 wie durch 6(1)(a) des Criminal Justice Act 2006 geändert, oder zur Ergreifung von Maßnahmen, um Strafverfolgungsbehörden Informationen zu melden, sofern erforderlich. Verbraucherangelegenheiten: zur Erfüllung unserer Verpflichtungen im Rahmen von Verbrauchergesetzen wie dem Competition and Consumer Protection Act 2014. Unternehmens- und Steuerangelegenheiten: zur Erfüllung unserer Verpflichtungen wie dem Companies Act 2014. Aufsichtsrechtliche Angelegenheiten: zur Erfüllung unserer Verpflichtungen zur Interaktion mit Aufsichtsbehörden, z. B. dem Data Protection Commission, im Rahmen der Datenschutz-Grundverordnung und des Data Protection Act 2018. Finanzangelegenheiten: zur Erfüllung unserer Verpflichtungen im Rahmen geltender Gesetze für Finanzdienstleistungen wie der European Union (Payment Services) Regulations 2018. Sieh die aktuelle Liste der Gesetze an, die in Irland durchsetzbar sind und durch die eine rechtliche Verpflichtung für Meta entsteht, welche zur Verarbeitung von Informationen führt. Durch neue Gesetze, die erlassen werden, oder andere Verpflichtungen, die für unsere Verarbeitung deiner Informationen verbindlich werden, sind wir unter Umständen zur Verarbeitung deiner Informationen verpflichtet, und wir werden diese Liste von Zeit zu Zeit aktualisieren. Die Informationskategorien hängen von den jeweiligen Umständen jeder verpflichtenden Anfrage oder Verpflichtung ab. Es werden nur die Informationen verarbeitet, die zur Erfüllung der entsprechenden rechtlichen Verpflichtungen erforderlich sind. Beispiel: Bei Zivilsachen sind dies in der Regel eingeschränkte Informationen (wie Kontaktdaten und Login-Informationen). Je nach den Umständen können jedoch auch folgende Kategorien dazugehören: Deine Aktivität und die von dir bereitgestellten Informationen: Inhalte, die du erstellst, wie Beiträge oder Kommentare oder Audio, Inhalte, die du über unsere Kamerafunktion oder deine Einstellungen für Aufnahmen oder über unsere sprachgestützten Funktionen bereitstellst, Nachrichten, die du sendest und empfangst, einschließlich ihrer Inhalte, vorbehaltlich des anwendbaren Rechts, Metadaten zu Inhalten und Nachrichten, Die Arten von Inhalten, die du dir ansiehst bzw. mit denen du interagierst, Die Apps und Funktionen, die du nutzt, und welche Handlungen du in ihnen durchführst, Käufe, die du tätigt, oder andere Transaktionen, die du durchführst, einschließlich gekürzter Kreditkartendaten, Hashtags, die du verwendest, Den Zeitpunkt, die Häufigkeit und die Dauer deiner Aktivitäten auf unseren Produkten, Freunde, Follower und andere Kontakte, App-, Browser- und Geräteinformationen: Geräteeigenschaften und Gerätesoftware, Was du gerade auf deinem Gerät tust (z. B. ob sich unsere

App im Vordergrund befindet oder ob sich deine Maus bewegt), Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, Gerätesignale, Informationen, die du über deine Geräteeinstellungen geteilt hast, Informationen zum Netzwerk, mit dem du dein Gerät verbindest, einschließlich deiner IP-Adresse, Informationen von Cookies und ähnlichen Technologien, Informationen von Partnern, Anbietern und Dritten. Berechtigte Interessen. Wir stützen uns auf unsere berechtigten Interessen bzw. die berechtigten Interessen eines Dritten, sofern nicht deine Interessen oder Grundrechte und Grundfreiheiten überwiegen („berechtigte Interessen“). Im Folgenden werden die verwendeten Informationskategorien dargelegt, auf welche berechtigten Interessen wir uns stützen sowie warum und wie die Daten verarbeitet werden: Wenn du ein registrierter Nutzer der Meta-Produkte bist. In Bezug auf Personen, die nicht volljährig (in den meisten betreffenden Ländern unter 18 Jahre) sind und nur beschränkt geschäftsfähig in Bezug auf den Abschluss eines durchsetzbaren Vertrags sind, können wir deine Informationen möglicherweise nicht aus Gründen der Erforderlichkeit für die Vertragserfüllung verarbeiten. Personalisierung der Meta-Produkte: Unsere Systeme verarbeiten automatisch Informationen, die wir im Zusammenhang mit dir und anderen Personen erhoben und gespeichert haben, um deine Interessen und Präferenzen zu bewerten und zu verstehen und dir über die Meta-Produkte hinweg gemäß unseren Nutzungsbedingungen personalisierte Erlebnisse zu bieten. Auf diese Weise: personalisieren wir Funktionen und Inhalte (wie deinen News Feed, Instagram-Feed und Stories), personalisieren wir die Werbeanzeigen, die den Nutzern angezeigt werden, und können wir dir auf unseren Produkten bzw. außerhalb dieser Vorschläge unterbreiten (z. B. Personen, die du kennen könntest, Gruppen oder Veranstaltungen, für die du dich interessieren könntest, oder Themen, die du eventuell abonnieren möchtest). Erfahre mehr dazu, wie wir Informationen über dich verwenden, um dein Erlebnis in und auf den Meta-Produkten zu personalisieren, und wie wir die Werbeanzeigen auswählen, die dir angezeigt werden. Um innovative Produkte und Funktionen zu erstellen, bereitzustellen, zu unterstützen und zu erhalten, die es Minderjährigen ermöglichen, sich auszudrücken, zu kommunizieren und für sie interessante Informationen und Gemeinschaften zu entdecken und damit zu interagieren, Gemeinschaften zu bilden und Tools und Funktionen zu nutzen, die ihr Wohlbefinden fördern. Um wichtige Updates im Zusammenhang mit unseren Produkten mit unseren nicht volljährigen Nutzern zu teilen und unsere Produkte und Dienste zu bewerben. Um die Meta-Produkte auf einheitliche Weise bereitzustellen, zu personalisieren und zu verbessern und gleichzeitig zusätzliche Schutzmaßnahmen für Personen bereitzustellen, die noch nicht das Alter der Einwilligungsfähigkeit des jeweiligen Mitgliedsstaats erreicht haben. Das berechtigte Interesse unserer Nutzer, in der Lage zu sein, auf die Meta-Produkte zuzugreifen und dass diese Produkte für jeden Nutzer personalisiert werden. Deine Aktivität und die von dir bereitgestellten Informationen: Inhalte, die du erstellst, wie Beiträge oder Kommentare oder Audio, Inhalte, die du über unsere Kamerafunktion oder deine Einstellungen für Aufnahmen oder über unsere sprachgestützten Funktionen bereitstellst, Metadaten zu Inhalten, Die Arten von Inhalten, die du dir ansiehst bzw. mit denen du interagierst, Die Apps und Funktionen, die du nutzt, und welche Handlungen du in ihnen durchführst, Käufe oder andere Transaktionen, die du ausführst, Hashtags, die du verwendest, Den Zeitpunkt, die Häufigkeit und die Dauer deiner Aktivitäten auf unseren Produkten, Freunde, Follower und andere Kontakte, App-, Browser- und Geräteinformationen: Geräteeigenschaften und Gerätesoftware, Was du gerade auf deinem Gerät tust (z. B. ob sich unsere App im Vordergrund befindet oder ob sich deine Maus bewegt), Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, Gerätesignale, Informationen, die du über deine Geräteeinstellungen geteilt hast (wie GPS-Standort), Informationen zum Netzwerk, mit dem du dein Gerät verbindest, Berichte über die Performance unserer Produkte auf deinem Gerät, Informationen von Cookies und ähnlichen Technologien, Informationen von Partnern, Anbietern und Dritten (außer Verwendung von Partnerdaten, um Werbung auf dich zuzuschneiden). Bereitstellung und Verbesserung unserer Meta-Produkte: Die Bereitstellung der Meta-Produkte umfasst die Erhebung, das Speichern und ggf. Teilen, Profiling, Überprüfen und Kuratieren, die automatisierte Verarbeitung und in einigen Fällen das manuelle (menschliche) Überprüfen, um: dein Konto und Profil zu erstellen und zu verwalten, das Teilen von Inhalten und Status zu ermöglichen, Funktionen bereitzustellen und zu kuratieren, Messaging-Dienste bereitzustellen sowie die Möglichkeit, Sprach- und Videoanrufe zu tätigen und sich mit anderen zu verbinden, Werbeprodukte bereitzustellen und Analysen durchzuführen. Wir verwenden Informationen, die uns vorliegen, auch, um Verbesserungen an unseren Produkten zu entwickeln, zu erforschen und zu testen. Wir verwenden die von uns erhobenen Informationen zu folgenden Zwecken: Sehen, ob ein Produkt ordnungsgemäß funktioniert, Nach Fehlern suchen und diese gegebenenfalls beheben, Neue Produkte und Funktionen testen, um deren Funktionalität zu prüfen, Feedback zu unseren Ideen für Produkte oder Funktionen einholen, Umfragen und andere Studien dazu durchführen, was dir an unseren Produkten und Marken gefällt und was wir noch besser machen können. Deine Aktivität und die von dir bereitgestellten Informationen: Inhalte, die du erstellst, wie Beiträge oder Kommentare oder Audio, Inhalte, die du über unsere Kamerafunktion oder deine Einstellungen für Aufnahmen oder über unsere sprachgestützten

Funktionen bereitstellst, Nachrichten, die du sendest und empfängst, einschließlich ihrer Inhalte, vorbehaltlich des anwendbaren Rechts, Metadaten zu Inhalten und Nachrichten, Die Arten von Inhalten, die du dir ansiehst bzw. mit denen du interagierst, Die Apps und Funktionen, die du nutzt, und welche Handlungen du in ihnen durchführst, Käufe, die du tätigtst, oder andere Transaktionen, die du durchführst, einschließlich gekürzter Kreditkartendaten, Hashtags, die du verwendest, Den Zeitpunkt, die Häufigkeit und die Dauer deiner Aktivitäten auf unseren Produkten, Freunde, Follower und andere Kontakte, App-, Browser- und Geräteinformationen: Geräteeigenschaften und Gerätesoftware, Was du gerade auf deinem Gerät tust (z. B. ob sich unsere App im Vordergrund befindet oder ob sich deine Maus bewegt), Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, Gerätesignale, Informationen, die du über deine Geräteeinstellungen geteilt hast, Informationen zum Netzwerk, mit dem du dein Gerät verbindest, einschließlich deiner IP-Adresse, Informationen von Cookies und ähnlichen Technologien, Informationen von Partnern, Anbietern und Dritten. Förderung von Schutz, Integrität und Sicherheit in und auf den Meta-Produkten: Die Meta-Produkte sollen dazu beitragen, den Schutz, die Integrität und die Sicherheit dieser Dienste und der Menschen, die sie nutzen, sicherzustellen. Wir verarbeiten Informationen, die wir mit dir verknüpft haben, und wenden dabei automatisierte Verarbeitungstechniken an und führen in einigen Fällen eine manuelle (menschliche) Überprüfung durch, um: Konten und Aktivitäten zu verifizieren, Verstöße gegen unsere Nutzungsbedingungen oder Richtlinien zu ermitteln und zu verfolgen. In einigen Fällen werden die von uns zu Verstößen getroffenen Entscheidungen vom Oversight Board überprüft, verdächtige Aktivitäten zu untersuchen, schädliches oder rechtswidriges Verhalten zu erkennen, zu verhindern und zu bekämpfen, z. B. durch Überprüfen und in einigen Fällen Entfernen von Inhalten, die uns gemeldet wurden, Spam und andere negative Erlebnisse aufzudecken und zu verhindern, Bedrohungen unseres Personals bzw. Eigentums aufzudecken und zu unterbinden, und die Integrität unserer Produkte zu wahren. Um weitere Informationen zu Schutz, Integrität und Sicherheit im Allgemeinen im Zusammenhang mit den Meta-Produkten zu erhalten, besuche den Facebook-Sicherheitsbereich und die Instagram-Sicherheitstipps. Um unsere Plattform und unser Netzwerk zu sichern, Konten und Aktivitäten zu verifizieren, schädliches Verhalten zu bekämpfen, Spam und andere negative Erlebnisse aufzudecken, zu verhindern und zu beheben, die Meta-Produkte von schädlichen oder unangemessenen Inhalten freizuhalten, verdächtige Aktivitäten oder Verstöße gegen unsere Nutzungsbedingungen oder Richtlinien zu untersuchen und um den Schutz von Minderjährigen sicherzustellen, u. a., um sie vor Ausbeutung oder sonstigen Schäden zu schützen, für die solche Personen eventuell besonders anfällig sind. Im Interesse unserer Nutzer und der allgemeinen Öffentlichkeit, um negative Erlebnisse zu verhindern und den Schutz, die Integrität und die Sicherheit sicherzustellen. Deine Aktivität und die von dir bereitgestellten Informationen: Inhalte, die du erstellst, wie Beiträge oder Kommentare oder Audio, Inhalte, die du über unsere Kamerafunktion oder deine Einstellungen für Aufnahmen oder über unsere sprachgestützten Funktionen bereitstellst, Nachrichten, die du sendest und empfängst, einschließlich ihrer Inhalte, vorbehaltlich des anwendbaren Rechts, Metadaten zu Inhalten und Nachrichten, Die Arten von Inhalten, die du dir ansiehst bzw. mit denen du interagierst, Die Apps und Funktionen, die du nutzt, und welche Handlungen du in ihnen durchführst, Käufe, die du tätigtst, oder andere Transaktionen, die du durchführst, einschließlich gekürzter Kreditkartendaten, Hashtags, die du verwendest, Den Zeitpunkt, die Häufigkeit und die Dauer deiner Aktivitäten auf unseren Produkten, Freunde, Follower und andere Kontakte App-, Browser- und Geräteinformationen: Geräteeigenschaften und Gerätesoftware, Was du gerade auf deinem Gerät tust (z. B. ob sich unsere App im Vordergrund befindet oder ob sich deine Maus bewegt), Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, Gerätesignale, Informationen, die du über deine Geräteeinstellungen geteilt hast, Informationen zum Netzwerk, mit dem du dein Gerät verbindest, einschließlich deiner IP-Adresse, Informationen von Cookies und ähnlichen Technologien, Informationen von Partnern, Anbietern und Dritten. Um wichtige Updates im Zusammenhang mit unseren Produkten mit unseren nicht volljährigen Nutzern zu teilen und unsere Produkte und Dienste zu bewerben. Deine Aktivität und die von dir bereitgestellten Informationen: Kontaktinformationen in deinem Profil und deine Kommunikation mit uns, Inhalte, die du erstellst, wie Beiträge oder Kommentare oder Audio, Inhalte, die du über unsere Kamerafunktion oder deine Einstellungen für Aufnahmen oder über unsere sprachgestützten Funktionen bereitstellst. App-, Browser- und Geräteinformationen: Geräteeigenschaften und Gerätesoftware, Was du gerade auf deinem Gerät tust (z. B. ob sich unsere App im Vordergrund befindet oder ob sich deine Maus bewegt), Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, Gerätesignale, Informationen, die du über deine Geräteeinstellungen geteilt hast, Informationen zum Netzwerk, mit dem du dein Gerät verbindest, einschließlich deiner IP-Adresse, Informationen von Cookies und ähnlichen Technologien. In Bezug auf alle Personen, einschließlich Minderjähriger: Bereitstellung von Messungen, Analysen und anderen Business-Services für Unternehmen, Werbetreibende und andere Partner: Unsere Systeme verarbeiten automatisch, sowie teilweise durch manuelle (menschliche) Verarbeitung, Informationen,

die wir über dich und andere erhoben und gespeichert haben. Wir verwenden diese Informationen, um: Unternehmen, Werbetreibenden und anderen Partnern Einblicke und Messberichten zur Verfügung zu stellen, um ihnen zu helfen, die Effektivität und Verbreitung ihrer Werbeanzeigen, Inhalte und Dienste oder der ihrer Kunden zu messen, um zu verstehen, welche Art von Personen ihre Inhalte und Werbeanzeigen sehen, und die Performance ihrer Inhalte und Werbeanzeigen auf und außerhalb von den Meta-Produkten nachzuvollziehen, und aggregierte Nutzeranalysen und Erkenntnisberichte bereitzustellen, die Unternehmen, Werbetreibenden und anderen Partnern helfen, die Zielgruppen, mit denen sie in Verbindung treten möchten, besser zu verstehen, sowie die Arten von Menschen, die ihre Dienste nutzen und wie Personen mit ihren Websites, Apps und Diensten interagieren. In unserem Interesse, um genaue und zuverlässige Berichte für unsere Werbetreibenden, Entwickler und sonstigen Partner bereitzustellen, um eine genaue Preisgestaltung und genaue Leistungsstatistiken sicherzustellen, und um den Wert aufzuzeigen, den unsere Partner durch die Nutzung der Produkte der Meta-Unternehmen realisieren; und im Interesse von Werbekunden, Entwicklern und sonstigen Partnern, um ihnen zu helfen, Erkenntnisse über ihre Kunden zu erlangen und Ihre Geschäfte zu verbessern, unsere Preismodelle zu validieren und die Effektivität ihrer Online-Inhalte und Werbung auf und außerhalb von den Produkten der Meta-Unternehmen zu bewerten. Deine Aktivität und die von dir bereitgestellten Informationen: Inhalte, die du erstellst, wie Beiträge oder Kommentare oder Audio, Inhalte, die du über unsere Kamerafunktion oder deine Einstellungen für Aufnahmen oder über unsere sprachgestützten Funktionen bereitstellst: Die Arten von Inhalten, die du dir ansiehst bzw. mit denen du interagierst, Die Apps und Funktionen, die du nutzt, und welche Handlungen du in ihnen durchführst, Käufe oder andere Transaktionen, die du ausführst, Hashtags, die du verwendest, Den Zeitpunkt, die Häufigkeit und die Dauer deiner Aktivitäten auf unseren Produkten, Freunde, Follower und andere Kontakte. App-, Browser- und Geräteinformationen: Geräteeigenschaften und Gerätesoftware, Was du gerade auf deinem Gerät tust (z. B. ob sich unsere App im Vordergrund befindet oder ob sich deine Maus bewegt), Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, Gerätesignale, Informationen, die du über deine Geräteeinstellungen geteilt hast, Informationen zum Netzwerk, mit dem du dein Gerät verbindest, einschließlich deiner IP-Adresse, Informationen von Cookies und ähnlichen Technologien, Informationen von Partnern, Anbietern und Dritten. Kommunikation, Interaktion und Teilen von Inhalten über die Produkte der Meta-Unternehmen hinweg: Um ein nahtloses, einheitliches und reichhaltigeres, innovatives Erlebnis über die Produkte der Meta-Unternehmen hinweg bereitzustellen und Interaktionen über verschiedene Apps hinweg sowie das Teilen, Anzeigen und Interagieren mit Inhalten, einschließlich Posts und Videos, zu ermöglichen. In unserem Interesse, um nahtlose, einheitliche und reichhaltigere, innovative Erlebnisse der Kommunikation, Interaktion und des Teilens von Inhalten über die Produkte der Meta-Unternehmen hinweg zu ermöglichen. Deine Aktivität und die von dir bereitgestellten Informationen: Inhalte, die du erstellst, wie Beiträge oder Kommentare oder Audio, Inhalte, die du über unsere Kamerafunktion oder deine Einstellungen für Aufnahmen oder über unsere sprachgestützten Funktionen bereitstellst, Metadaten zu Inhalten, Die Arten von Inhalten, die du dir ansiehst bzw. mit denen du interagierst, Die Apps und Funktionen, die du nutzt, und welche Handlungen du in ihnen durchführst, Käufe oder andere Transaktionen, die du ausführst, Hashtags, die du verwendest, Den Zeitpunkt, die Häufigkeit und die Dauer deiner Aktivitäten auf unseren Produkten, Freunde, Follower und andere Kontakte. App-, Browser- und Geräteinformationen: Geräteeigenschaften und Gerätesoftware, Was du gerade auf deinem Gerät tust (z. B. ob sich unsere App im Vordergrund befindet oder ob sich deine Maus bewegt), Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, Gerätesignale, Informationen, die du über deine Geräteeinstellungen geteilt hast, Informationen zum Netzwerk, mit dem du dein Gerät verbindest, einschließlich deiner IP-Adresse, Informationen von Cookies und ähnlichen Technologien, Informationen von Partnern, Anbietern und Dritten. Business Intelligence und Statistik: Um in aggregierter Form deine Nutzung unserer Produkte und über diese hinweg zu verstehen, um Personen und Unternehmen richtig zählen zu können und Kennzahlen im Zusammenhang damit zu bestätigen, um zu informieren und die Produktrichtung und -entwicklung zu verbessern, und um Berichtspflichten (gegenüber Aktionären/hinsichtlich Gewinnen) nachzukommen. In unserem Interesse, um die Nutzung unserer Produkte und Dienste zu messen und die Personen zu zählen, die mit unseren Produkten und Diensten interagieren, um zu informieren und die Produktrichtung und -entwicklung zu verbessern und um die Bereitstellung richtiger und zuverlässiger Berichte sicherzustellen. Deine Aktivität und die von dir bereitgestellten Informationen: Inhalte, die du erstellst, wie Beiträge oder Kommentare oder Audio, Inhalte, die du über unsere Kamerafunktion oder deine Einstellungen für Aufnahmen oder über unsere sprachgestützten Funktionen bereitstellst, Metadaten zu Inhalten und Nachrichten, Die Arten von Inhalten, die du dir ansiehst bzw. mit denen du interagierst, Die Apps und Funktionen, die du nutzt, und welche Handlungen du in ihnen durchführst, Käufe oder andere Transaktionen, die du ausführst, Hashtags, die du verwendest, Den Zeitpunkt, die Häufigkeit und die Dauer deiner Aktivitäten auf unseren Produkten, Freunde, Follower und andere

Kontakte. App-, Browser- und Geräteinformationen: Geräteeigenschaften und Gerätesoftware, Was du gerade auf deinem Gerät tust (z. B. ob sich unsere App im Vordergrund befindet oder ob sich deine Maus bewegt), Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, Gerätesignale, Informationen, die du über deine Geräteeinstellungen geteilt hast, Informationen zum Netzwerk, mit dem du dein Gerät verbindest, einschließlich deiner IP-Adresse, Informationen von Cookies und ähnlichen Technologien, Informationen von Partnern, Anbietern und Dritten. Identifizieren deiner Person als Nutzer von Meta-Produkten und Personalisieren der Anzeigen, die wir dir über das Meta Audience Network zeigen, wenn du andere Apps besuchst: Wenn wir dir über Meta Audience Network Anzeigen zeigen, wenn du andere Apps besuchst, verarbeiten unsere Systeme automatisch die Informationen, die wir über dich und andere erhoben und gespeichert haben, um dich als Nutzer von Meta-Produkten zu identifizieren und die dir angezeigte Werbung auf dich zuzuschneiden. In unserem Interesse zur Finanzierung unserer Bereitstellung der Meta-Produkte und zur Bereitstellung von qualitativ hochwertigen, personalisierten Werbeanzeigen an Nutzer, die die Websites, Apps und Geräte besuchen, die unsere Werbedienste nutzen; In unserem Interesse zum Hervorheben der Meta-Produkte für Personen, die keine registrierten Nutzer der Meta-Produkte sind; und Im Interesse von Werbetreibenden, die Personen erreichen möchten, die an ihren Informationen, Produkten oder Diensten interessiert sein könnten. Deine Aktivität und die von dir bereitgestellten Informationen: Inhalte, die du erstellst, wie Beiträge oder Kommentare oder Audio, Inhalte, die du über unsere Kamerafunktion oder deine Einstellungen für Aufnahmen oder über unsere sprachgestützten Funktionen bereitstellst, Metadaten zu Inhalten, Die Arten von Inhalten, die du dir ansiehst bzw. mit denen du interagierst, Die Apps und Funktionen, die du nutzt, und welche Handlungen du in ihnen durchführst, Käufe oder andere Transaktionen, die du ausführst, Hashtags, die du verwendest, Den Zeitpunkt, die Häufigkeit und die Dauer deiner Aktivitäten auf unseren Produkten, Freunde, Follower und andere Kontakte. App-, Browser- und Geräteinformationen: Geräteeigenschaften und Gerätesoftware, Was du gerade auf deinem Gerät tust (z. B. ob sich unsere App im Vordergrund befindet oder ob sich deine Maus bewegt), Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, Gerätesignale, Informationen, die du über deine Geräteeinstellungen geteilt hast, Informationen zum Netzwerk, mit dem du dein Gerät verbindest, einschließlich deiner IP-Adresse, Informationen von Cookies und ähnlichen Technologien. Informationen von Partnern, Anbietern und Dritten. Erhalten und Verwenden von Informationen von einem bestimmten Unternehmen, um die dir gezeigten Werbeanzeigen auf dich zuzuschneiden: Wir verwenden Informationen von einem bestimmten Unternehmen, das eine Liste der Personen oder Geräte mit uns geteilt hat, wenn wir in deinem Profil ein Match mit den Informationen auf dieser Liste finden, um die Werbung, die wir dir auf Meta-Produkten anzeigen, auf dich zuzuschneiden, unter anderem durch Meta Audience Network. In unserem Interesse zur Finanzierung unserer Bereitstellung der Meta-Produkte und zur Bereitstellung von qualitativ hochwertigen, personalisierten Werbeanzeigen an Nutzer, die die Websites, Apps und Geräte besuchen, die unsere Werbedienste nutzen; und im Interesse von Werbetreibenden, die Personen erreichen möchten, die an ihren Informationen, Produkten oder Diensten interessiert sein könnten. Deine Aktivität und die von dir bereitgestellten Informationen: Informationen und Inhalte, die du bereitstellst, wie z. B. deinen Namen oder deine E-Mail-Adresse. Informationen von Partnern, Anbietern und Dritten. Bereitstellen von Marketing-Kommunikation für dich: Je nach deinen Einstellungen senden wir dir von Zeit zu Zeit Marketing-Kommunikation. Wir erheben und speichern deine Informationen und verwenden sie, um dir Marketing-Kommunikation zu senden, wie z. B. eine E-Mail. In unserem Interesse, die Produkte der Meta-Unternehmen zu fördern, und unser Direktmarketing zu versenden. Deine Aktivität und die von dir bereitgestellten Informationen: Informationen und Inhalte, die du zur Verfügung stellst, einschließlich deiner Kontaktinformationen wie z. B. deine E-Mail-Adresse. App-, Browser- und Geräteinformationen: Geräte-IDs. Forschung und Innovation für soziale Zwecke: Wir führen Umfragen durch und verwenden Informationen (u. a. von Forschern, mit denen wir zusammenarbeiten), um Forschung und Innovation zu Themen des sozialen Allgemeinwohls, des technologischen Fortschritts, des öffentlichen Interesses, der Gesundheit und des Wohlergehens durchzuführen und zu unterstützen. Beispielsweise analysieren wir die uns über Migrationsmuster in Krisensituationen zur Verfügung stehenden Informationen. Dies unterstützt Hilfsorganisationen dabei, Hilfsmittel und Unterstützung an die richtigen Orte zu bringen. Wir erheben, speichern, verknüpfen, analysieren und wenden automatische Verarbeitungstechniken wie Aggregation von Daten sowie manuelle (menschliche) Überprüfungen an und teilen Informationen, um auf diese Weise Forschung zu betreiben und Innovationen für soziale Zwecke zu fördern. Wir tun dies, um beispielsweise COVID-19-Prognosemodelle zu erstellen. Mehr zu unseren Forschungsprogrammen. In unserem Interesse und im Interesse der allgemeinen Öffentlichkeit, um den Stand der Technik bzw. das wissenschaftliche Verständnis bezüglich wichtiger sozialer Themen zu fördern, die unsere Gesellschaft und Welt positiv beeinflussen. Deine Aktivität und die von dir bereitgestellten Informationen: Inhalte, die du erstellst, wie Beiträge oder Kommentare oder Audio, Inhalte, die du über unsere Kamerafunktion oder deine

Einstellungen für Aufnahmen oder über unsere sprachgestützten Funktionen bereitstellt, Metadaten zu Inhalten und Nachrichten, Die Arten von Inhalten, die du dir ansiehst bzw. mit denen du interagierst, Die Apps und Funktionen, die du nutzt, und welche Handlungen du in ihnen durchführst, Käufe oder andere Transaktionen, die du ausführst, Hashtags, die du verwendest, Den Zeitpunkt, die Häufigkeit und die Dauer deiner Aktivitäten auf unseren Produkten, Freunde, Follower und andere Kontakte. App-, Browser- und Geräteinformationen: Geräteeigenschaften und Gerätesoftware, Was du gerade auf deinem Gerät tust (z. B. ob sich unsere App im Vordergrund befindet oder ob sich deine Maus bewegt), Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, Gerätesignale, Informationen, die du über deine Geräteeinstellungen geteilt hast, Informationen zum Netzwerk, mit dem du dein Gerät verbindest, einschließlich deiner IP-Adresse, Informationen von Cookies und ähnlichen Technologien. Informationen von Partnern, Anbietern und Dritten.

Anonymisieren deiner Informationen: In einigen Fällen anonymisieren wir Informationen, die uns über dich vorliegen, z. B. deine Aktivität auf und außerhalb von unseren Produkten, und nutzen die daraus resultierenden Informationen beispielsweise, um unsere Meta-Produkte, einschließlich Werbeanzeigen, bereitzustellen und zu verbessern. In unserem Interesse zur Finanzierung unserer Bereitstellung der Meta-Produkte, Bereitstellung relevanter Werbung für Nutzer und Verbesserung der Anzeigenauslieferung und Meta-Produkte; Im Interesse von Werbetreibenden, um ihnen zu helfen, relevante Zielgruppen, die an ihren Informationen, Produkten oder Diensten interessiert sein könnten, zu erreichen; Im Interesse von Nutzern, damit Meta Datenminimierung und eingebauten Datenschutz in Bezug auf ihre Informationen praktizieren kann. Deine Aktivität und die von dir bereitgestellten Informationen: Inhalte, die du erstellst, wie Beiträge oder Kommentare oder Audio, Inhalte, die du über unsere Kamerafunktion oder deine Einstellungen für Aufnahmen oder über unsere sprachgestützten Funktionen bereitstellt, Metadaten zu Inhalten, Die Arten von Inhalten, die du dir ansiehst bzw. mit denen du interagierst, Die Apps und Funktionen, die du nutzt, und welche Handlungen du in ihnen durchführst, Käufe oder andere Transaktionen, die du ausführst, Hashtags, die du verwendest, Den Zeitpunkt, die Häufigkeit und die Dauer deiner Aktivitäten auf unseren Produkten, Freunde, Follower und andere Kontakte. App-, Browser- und Geräteinformationen: Geräteeigenschaften und Gerätesoftware, Was du gerade auf deinem Gerät tust (z. B. ob sich unsere App im Vordergrund befindet oder ob sich deine Maus bewegt), Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, Gerätesignale, Informationen, die du über deine Geräteeinstellungen geteilt hast, Informationen zum Netzwerk, mit dem du dein Gerät verbindest, einschließlich deiner IP-Adresse, Informationen von Cookies und ähnlichen Technologien. Informationen von Partnern, Anbietern und Dritten. Weitergabe von Informationen an andere, einschließlich Strafverfolgungsbehörden, und um auf rechtliche Anfragen zu reagieren. Informationen darüber, wie wir Informationen an Strafverfolgungsbehörden und andere weitergeben, findest du unter Wie reagieren wir auf rechtliche Anfragen, verhindern Schäden und fördern den Schutz und die Sicherheit? Die Kategorien von Informationen, auf die wir zugreifen, die wir aufbewahren, nutzen und teilen, hängen von den jeweiligen Umständen ab. Beispiel: Bei Reaktionen auf rechtliche Anfragen, zu denen wir gesetzlich nicht verpflichtet sind, sind dies in der Regel eingeschränkte Informationen (wie Kontaktdaten und Login-Informationen). Die Informationen, die wir verarbeiten, hängen jedoch von den Verarbeitungszwecken ab, zu denen folgende gehören können: als Reaktion auf rechtliche Anfragen von Dritten wie zum Beispiel von Prozessführenden in Zivilprozessen oder von Strafverfolgungs- und anderen Behörden: um anwendbares Recht einzuhalten oder legitime rechtliche Zwecke zu erfüllen, um den Schutz, die Sicherheit und die Integrität von Meta, Meta-Produkten, Produkten, der Nutzer, der Mitarbeiter, des Eigentums und der Öffentlichkeit sicherzustellen. Erfahre mehr dazu, wie wir Schutz, Integrität und Sicherheit fördern. In unserem Interesse und im Interesse der allgemeinen Öffentlichkeit, um Betrug, eine unberechtigte Nutzung der Produkte der Meta-Unternehmen, Verstöße gegen unsere Nutzungsbedingungen oder Richtlinien sowie sonstige schädliche oder illegale Aktivitäten zu verhindern und zu verfolgen; um uns (einschließlich unserer Rechte, des Personals und des Eigentums von Meta bzw. der Meta-Produkte), unsere Nutzer oder andere zu schützen, u. a. im Rahmen von Untersuchungen oder Auskunftersuchen der Aufsichtsbehörden; oder um den Tod oder eine drohende Körperverletzung zu verhindern. Deine Aktivität und die von dir bereitgestellten Informationen: Inhalte, die du erstellst, wie Beiträge oder Kommentare oder Audio, Inhalte, die du über unsere Kamerafunktion oder deine Einstellungen für Aufnahmen oder über unsere sprachgestützten Funktionen bereitstellt, Metadaten zu Inhalten, Die Arten von Inhalten, die du dir ansiehst bzw. mit denen du interagierst, Die Apps und Funktionen, die du nutzt, und welche Handlungen du in ihnen durchführst, Käufe oder andere Transaktionen, die du ausführst, Hashtags, die du verwendest, Freunde, Follower und andere Kontakte. App-, Browser- und Geräteinformationen: Geräteeigenschaften und Gerätesoftware, Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, Gerätesignale, Informationen, die du über deine Geräteeinstellungen geteilt hast, Informationen zum Netzwerk, mit dem du dein Gerät verbindest, einschließlich deiner IP-Adresse, Informationen von Cookies und ähnlichen Technologien.

Informationen von Partnern, Anbietern und Dritten. Förderung des Schutzes, der Integrität und der Sicherheit unter bestimmten Umständen außerhalb der Erfüllung unserer Verträge mit dir: Unsere Meta-Produkte werden bereitgestellt, um den Schutz, die Integrität und die Sicherheit dieser Dienste und der Menschen, die sie nutzen, sicherzustellen. Wir führen automatisierte Verarbeitungen sowie manuelle (menschliche) Überprüfungen durch, um Konten und Aktivitäten zu verifizieren, schädliches Verhalten zu bekämpfen, Spam und sonstige Sicherheitsangelegenheiten sowie negative Erlebnisse anderer Art aufzudecken und zu verhindern, die Integrität unserer Produkte aufrechtzuerhalten und den Schutz, die Integrität und die Sicherheit auf und außerhalb der Meta-Produkte zu fördern. Zum Beispiel verwenden wir uns zur Verfügung stehende Informationen, um verdächtige Aktivitäten oder Verletzungen unserer Nutzungsbedingungen oder Richtlinien zu untersuchen oder um zu erkennen, wenn jemand Hilfe benötigt. Mehr dazu erfährst du im Facebook-Sicherheitsbereich und in den Instagram-Sicherheitstipps. In unserem Interesse, unsere Plattform und unser Netzwerk zu sichern, Konten und Aktivitäten zu verifizieren, schädliches Verhalten zu bekämpfen, Spam und andere negative Erlebnisse aufzudecken, zu verhindern und zu verfolgen, die Produkte der Meta-Unternehmen von schädlichen oder unangemessenen Inhalten freizuhalten und um verdächtige Aktivitäten oder Verstöße gegen unsere Nutzungsbedingungen oder Richtlinien zu untersuchen und diesbezüglich Maßnahmen zu ergreifen; und im Interesse unserer Nutzer und der allgemeinen Öffentlichkeit, um negative Erlebnisse zu verhindern und den Schutz, die Integrität und die Sicherheit sicherzustellen. Deine Aktivität und die von dir bereitgestellten Informationen: Inhalte, die du erstellst, wie Beiträge oder Kommentare oder Audio, Inhalte, die du über unsere Kamerafunktion oder deine Einstellungen für Aufnahmen oder über unsere sprachgestützten Funktionen bereitstellst, Metadaten zu Inhalten, Die Arten von Inhalten, die du dir ansiehst bzw. mit denen du interagierst, Die Apps und Funktionen, die du nutzt, und welche Handlungen du in ihnen durchführst, Käufe, die du tätigt, oder andere Transaktionen, die du durchführst, einschließlich gekürzter Kreditkartendaten, Hashtags, die du verwendest, Den Zeitpunkt, die Häufigkeit und die Dauer deiner Aktivitäten auf unseren Produkten. Freunde, Follower und andere Kontakte. App-, Browser- und Geräteinformationen: Geräteeigenschaften und Gerätesoftware, Was du gerade auf deinem Gerät tust (z. B. ob sich unsere App im Vordergrund befindet oder ob sich deine Maus bewegt), Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, Gerätesignale, Informationen, die du über deine Geräteeinstellungen geteilt hast, Informationen zum Netzwerk, mit dem du dein Gerät verbindest, einschließlich deiner IP-Adresse, Informationen von Cookies und ähnlichen Technologien.

Informationen von Partnern, Anbietern und Dritten. Wenn du ein Gerät benutzt, das wir nicht mit einem registrierten Nutzer der Meta-Produkte verknüpfen können. Förderung von Schutz, Integrität und Sicherheit: Unsere Meta-Produkte werden in einer Weise bereitgestellt, die den Schutz, die Integrität und die Sicherheit dieser Dienste und der Menschen, die sie nutzen, sicherstellen soll. Wir erheben und speichern Informationen, die uns zur Verfügung stehen, für diesen Zweck und führen automatisierte Verarbeitungen und manuelle (d. h. menschliche) Überprüfungen durch, um Konten und Aktivitäten zu verifizieren, schädliches Verhalten zu bekämpfen, Spam und sonstige Sicherheitsangelegenheiten sowie negative Erlebnisse anderer Art aufzudecken und zu verhindern, die Integrität unserer Produkte aufrechtzuerhalten und den Schutz, die Integrität und die Sicherheit auf und außerhalb der Meta-Produkte zu untersuchen und zu fördern. Zum Beispiel verwenden wir uns zur Verfügung stehende Informationen, um verdächtige Aktivitäten oder Verletzungen unserer Nutzungsbedingungen oder Richtlinien zu untersuchen oder um zu erkennen, wenn jemand Hilfe benötigt. Mehr dazu erfährst du im Facebook-Sicherheitsbereich und in den Instagram-Sicherheitstipps. In unserem Interesse, unsere Plattform und unser Netzwerk zu sichern, Konten und Aktivitäten zu verifizieren, schädliches Verhalten zu bekämpfen, Spam und andere negative Erlebnisse aufzudecken, zu verhindern und zu verfolgen, die Produkte der Meta-Unternehmen von schädlichen oder unangemessenen Inhalten freizuhalten und um verdächtige Aktivitäten oder Verstöße gegen unsere Nutzungsbedingungen oder Richtlinien zu untersuchen und diesbezüglich Maßnahmen zu ergreifen; und Im Interesse unserer Nutzer im Allgemeinen und der breiten Öffentlichkeit, um negative Erlebnisse zu verhindern und den Schutz, die Integrität und die Sicherheit zu fördern. Deine Aktivität und die von dir bereitgestellten Informationen: Die Arten von Inhalten, die du dir ansiehst bzw. mit denen du interagierst, Die Apps und Funktionen, die du nutzt, und welche Handlungen du in ihnen durchführst, Den Zeitpunkt, die Häufigkeit und die Dauer deiner Aktivitäten auf unseren Produkten. App-, Browser- und Geräteinformationen: Geräteeigenschaften und Gerätesoftware, Was du gerade auf deinem Gerät tust (z. B. ob sich unsere App im Vordergrund befindet oder ob sich deine Maus bewegt), Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, Gerätesignale, Informationen, die du über deine Geräteeinstellungen geteilt hast, Informationen zum Netzwerk, mit dem du dein Gerät verbindest, einschließlich deiner IP-Adresse, Informationen von Cookies und ähnlichen Technologien. Informationen von Partnern, Anbietern und Dritten. Bereitstellen von Marketing-Kommunikation für dich: Wir erheben und speichern deine Informationen, verwenden sie, um dir Marketing-Kommunikation zu senden, wie z. B.

eine E-Mail. In unserem Interesse, die Produkte der Meta-Unternehmen zu fördern, und unser Direktmarketing zu versenden. Deine Aktivität und die von dir bereitgestellten Informationen: Informationen und Inhalte, die du zur Verfügung stellst, einschließlich deiner Kontaktinformationen wie z. B. deiner E-Mail-Adresse. Forschung und Innovation für soziale Zwecke: Wir führen Umfragen durch und verwenden Informationen (u. a. von Forschungspartnern, mit denen wir zusammenarbeiten), um Forschung und Innovation zu Themen des sozialen Allgemeinwohls, des technologischen Fortschritts, des öffentlichen Interesses, der Gesundheit und des Wohlergehens durchzuführen und zu unterstützen. Wir erheben, speichern, verknüpfen, analysieren und wenden automatische Verarbeitungstechniken wie Aggregation auf Informationen sowie manuelle (menschliche) Überprüfungen im erforderlichen Maß an, um auf diese Weise Forschung zu betreiben und Innovationen für soziale Zwecke zu fördern. Mehr zu unseren Forschungsprogrammen. In unserem Interesse und im Interesse der allgemeinen Öffentlichkeit, um den Stand der Technik bzw. das wissenschaftliche Verständnis bezüglich wichtiger sozialer Themen zu fördern, die unsere Gesellschaft und Welt positiv beeinflussen. Deine Aktivität und die von dir bereitgestellten Informationen: Die Arten von Inhalten, die du dir ansiehst bzw. mit denen du interagierst, Die Apps und Funktionen, die du nutzt, und welche Handlungen du in ihnen durchführst, Den Zeitpunkt, die Häufigkeit und die Dauer deiner Aktivitäten auf unseren Produkten. App-, Browser- und Geräteinformationen: Geräteeigenschaften und Gerätesoftware, Was du gerade auf deinem Gerät tust (z. B. ob sich unsere App im Vordergrund befindet oder ob sich deine Maus bewegt), Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, Gerätesignale, Informationen, die du über deine Geräteeinstellungen geteilt hast, Informationen zum Netzwerk, mit dem du dein Gerät verbindest, einschließlich deiner IP-Adresse, Informationen von Cookies und ähnlichen Technologien. Informationen von Partnern, Anbietern und Dritten. Weitergabe von Informationen an andere, einschließlich Strafverfolgungsbehörden, und um auf rechtliche Anfragen zu reagieren. Informationen darüber, wie wir Informationen an Strafverfolgungsbehörden und andere weitergeben, findest du unter Wie reagieren wir auf rechtliche Anfragen, verhindern Schäden und fördern den Schutz und die Sicherheit? Die Kategorien von Informationen, auf die wir zugreifen, die wir aufbewahren, nutzen und teilen, hängen von den jeweiligen Umständen ab. Beispiel: Bei Reaktionen auf rechtliche Anfragen, zu denen wir gesetzlich nicht verpflichtet sind, sind dies in der Regel eingeschränkte Informationen (wie Kontaktdaten und Login-Informationen). Die Informationen, die wir verarbeiten, hängen jedoch von den Verarbeitungszwecken ab, zu denen folgende gehören können: als Reaktion auf rechtliche Anfragen von Dritten wie zum Beispiel von Prozessführenden in Zivilprozessen oder von Strafverfolgungs- und anderen Behörden: um anwendbares Recht einzuhalten oder legitime rechtliche Zwecke zu erfüllen, um den Schutz, die Sicherheit und die Integrität von Meta, Meta-Produkten, Produkten, der Nutzer, der Mitarbeiter, des Eigentums und der Öffentlichkeit sicherzustellen. Erfahre mehr dazu, wie wir Schutz, Integrität und Sicherheit fördern. In unserem Interesse und im Interesse der allgemeinen Öffentlichkeit, um Betrug, eine unberechtigte Nutzung der Produkte der Meta-Unternehmen, Verstöße gegen unsere Nutzungsbedingungen oder Richtlinien sowie sonstige schädliche oder illegale Aktivitäten zu verhindern und zu verfolgen; um uns (einschließlich unserer Rechte, des Personals und des Eigentums von Meta bzw. der Meta-Produkte), unsere Nutzer oder andere zu schützen, u. a. im Rahmen von Untersuchungen oder Auskunftersuchen der Aufsichtsbehörden; oder um den Tod oder eine drohende Körperverletzung zu verhindern. Deine Aktivität und die von dir bereitgestellten Informationen: Die Arten von Inhalten, die du dir ansiehst bzw. mit denen du interagierst, Die Apps und Funktionen, die du nutzt, und welche Handlungen du in ihnen durchführst, Den Zeitpunkt, die Häufigkeit und die Dauer deiner Aktivitäten auf unseren Produkten. App-, Browser- und Geräteinformationen: Geräteeigenschaften und Gerätesoftware, Was du gerade auf deinem Gerät tust (z. B. ob sich unsere App im Vordergrund befindet oder ob sich deine Maus bewegt), Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, Gerätesignale, Informationen, die du über deine Geräteeinstellungen geteilt hast, Informationen zum Netzwerk, mit dem du dein Gerät verbindest, einschließlich deiner IP-Adresse, Informationen von Cookies und ähnlichen Technologien. Informationen von Partnern, Anbietern und Dritten. Produktverbesserung: Wir verwenden die von uns erhobenen Informationen zu folgenden Zwecken: Sehen, ob ein Produkt ordnungsgemäß funktioniert, Nach Fehlern suchen und diese gegebenenfalls beheben, Neue Produkte und Funktionen testen, um deren Funktionalität zu prüfen, Feedback zu unseren Ideen für Produkte oder Funktionen einholen, Umfragen und andere Studien dazu durchführen, was dir an unseren Produkten und Marken gefällt und was wir noch besser machen können. Um die Produkte der Meta-Unternehmen auf einheitliche Weise zu verbessern, um technische Funktionsstörungen zu beheben und um die Funktionalität zu optimieren. App-, Browser- und Geräteinformationen: Geräteeigenschaften und Gerätesoftware, Was du gerade auf deinem Gerät tust (z. B. ob sich unsere App im Vordergrund befindet oder ob sich deine Maus bewegt), Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, Gerätesignale, Informationen, die du über deine Geräteeinstellungen geteilt hast, Informationen zum Netzwerk, mit

dem du dein Gerät verbindest, einschließlich deiner IP-Adresse, Informationen von Cookies und ähnlichen Technologien. Informationen von Partnern, Anbietern und Dritten. Wenn wir deine Informationen verarbeiten, weil dies notwendig ist, um unsere berechtigten Interessen oder die eines Dritten zu verfolgen, hast du das Recht, Widerspruch einzulegen und die Einschränkung der Verarbeitung zu beantragen. Um deine Rechte auszuüben, gehe zu den Facebook-Einstellungen, zum Hilfebereich und zu den Instagram-Einstellungen. Wir werden verschiedene Faktoren berücksichtigen, wenn wir einen Widerspruch bewerten, wie unter anderem: die vernünftigen Erwartungen unserer Nutzer; Nutzen und Risiken für dich, uns, andere Nutzer oder Dritte; sowie sonstige verfügbare Mittel zur Erreichung desselben Zwecks, die möglicherweise weniger invasiv sind und keinen unverhältnismäßigen Aufwand erfordern. Sofern wir nicht feststellen, dass wir zwingende berechnete Gründe für diese Verarbeitung haben, die deine Interessen oder Grundrechte und -freiheiten überwiegen, oder sofern die Verarbeitung nicht aus rechtlichen Gründen erforderlich ist, wird dein Widerspruch aufrechterhalten und wir werden die Verarbeitung deiner Daten einstellen. Weitere Informationen zu den Umständen, unter denen ein Widerspruch erfolgreich sein kann, findest du im Hilfebereich. Wenn du in deinem Land minderjährig bist und kein durchsetzbarer Vertrag besteht, werden wir die Tatsache, dass du minderjährig bist, besonders berücksichtigen, wenn wir unsere Bewertung unserer berechtigten Interessen sowie die Abwägung deiner Interessen und Rechte durchführen. Wir stellen Minderjährigen einen besonderen Schutz bereit, um sicherzustellen, dass sie sich der Risiken, Folgen, Garantien und Rechte bewusst sind, die mit der Verarbeitung ihrer Informationen verbunden sind. Im öffentlichen Interesse durchgeführte Aufgaben. Die Zwecke, für die wir die Verarbeitung deiner Informationen als Aufgabe im öffentlichen Interesse erwarten, die Verarbeitung, die wir vornehmen, und die Informationen, die wir verwenden, werden nachstehend dargelegt: Forschung für soziale Zwecke: Wir erheben, speichern, verknüpfen, analysieren und wenden automatische Verarbeitungstechniken wie Aggregation auf Informationen sowie manuelle (menschliche) Überprüfungen an, um auf diese Weise Forschung zu betreiben und andere Aufgaben zu erledigen, die im öffentlichen Interesse sind, beispielsweise Teilen relevanter Forschungsdaten mit Dritten wie internationalen Organisationen und Wissenschaftlern innerhalb und außerhalb des EWR. Das öffentliche Interesse muss in den Rechtsvorschriften der Union oder des Mitgliedstaats oder anderen relevanten Gesetzen, denen wir unterliegen, verankert sein. In diesem Fall stützen wir uns auf die Artikel 168 und 179 des Vertrags über die Arbeitsweise der Europäischen Union. Deine Aktivität und die von dir bereitgestellten Informationen: Inhalte, die du erstellst, wie Beiträge oder Kommentare oder Audio, Inhalte, die du über unsere Kamerafunktion oder deine Einstellungen für Aufnahmen oder über unsere sprachgestützten Funktionen bereitstellst, Metadaten zu Inhalten, Die Arten von Inhalten, die du dir ansiehst bzw. mit denen du interagierst, Die Apps und Funktionen, die du nutzt, und welche Handlungen du in ihnen durchführst, Käufe oder andere Transaktionen, die du ausführst, Hashtags, die du verwendest, Den Zeitpunkt, die Häufigkeit und die Dauer deiner Aktivitäten auf unseren Produkten, Freunde, Follower und andere Kontakte. App-, Browser- und Geräteinformationen: Geräteeigenschaften und Gerätesoftware, Was du gerade auf deinem Gerät tust (z. B. ob sich unsere App im Vordergrund befindet oder ob sich deine Maus bewegt), Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, Gerätesignale, Informationen, die du über deine Geräteeinstellungen geteilt hast, Informationen zum Netzwerk, mit dem du dein Gerät verbindest, einschließlich deiner IP-Adresse, Informationen von Cookies und ähnlichen Technologien. Informationen von Partnern, Anbietern und Dritten. Zur Förderung von Schutz, Integrität und Sicherheit: Unter spezifischen tatsächlichen Umständen greifen wir auf deine Daten zu, bewahren sie auf und geben sie an Aufsichtsbehörden, Strafverfolgungsbehörden oder andere weiter, wenn dies zur Erfüllung einer Aufgabe im öffentlichen Interesse erforderlich ist. So können wir beispielsweise Informationen mit anderen zum Zwecke der Bekämpfung rechtswidrigen oder schädlichen Verhaltens teilen, wenn dies im öffentlichen Interesse liegt und wenn das öffentliche Interesse im Unionsrecht oder im Recht der Mitgliedstaaten oder in anderen anwendbaren Gesetzen, denen wir unterliegen, festgelegt ist. In diesem Fall stützen wir uns auf Section 53 des Data Protection Act 2018 und auf die Verordnung (EU) 2021/1232. Deine Aktivität und die von dir bereitgestellten Informationen: Inhalte, die du erstellst, wie Beiträge oder Kommentare oder Audio. Inhalte, die du über unsere Kamerafunktion oder deine Einstellungen für Aufnahmen oder über unsere sprachgestützten Funktionen bereitstellst. Metadaten zu Inhalten. Die Arten von Inhalten, die du dir ansiehst bzw. mit denen du interagierst. Die Apps und Funktionen, die du nutzt, und welche Handlungen du in ihnen durchführst. Käufe, die du tätigst, oder andere Transaktionen, die du durchführst, einschließlich gekürzter Kreditkartendaten. Hashtags, die du verwendest. Den Zeitpunkt, die Häufigkeit und die Dauer deiner Aktivitäten auf unseren Produkten. Freunde, Follower und andere Kontakte. App-, Browser- und Geräteinformationen: Geräteeigenschaften und Gerätesoftware. Was du gerade auf deinem Gerät tust (z. B. ob sich unsere App im Vordergrund befindet oder ob sich deine Maus bewegt) Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, Gerätesignale, Informationen, die du über deine Geräteeinstellungen geteilt hast, Informationen zum Netzwerk, mit dem du dein

Gerät verbindest, einschließlich deiner IP-Adresse, Informationen von Cookies und ähnlichen Technologien, Informationen von Partnern, Anbietern und Dritten. Wenn wir deine Informationen so verarbeiten, wie es für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist, hast du das Recht, unserer Verarbeitung zu widersprechen und ihre Einschränkung zu verlangen. Um deine Rechte auszuüben, gehe zu den Facebook-Einstellungen, zum Hilfebereich und den Instagram-Einstellungen. Bei der Bewertung eines Widerspruchs werden wir verschiedene Faktoren berücksichtigen, wie unter anderem: die vernünftigen Erwartungen unserer Nutzer; Nutzen und Risiken für dich, uns, andere Nutzer oder Dritte; sowie sonstige verfügbare Mittel zur Erreichung desselben Zwecks, die möglicherweise weniger invasiv sind und keinen unverhältnismäßigen Aufwand erfordern. Dein Widerspruch wird aufrechterhalten, und wir werden die Verarbeitung deiner Daten einstellen, es sei denn, wir stellen fest, dass wir zwingende berechnete Gründe für diese Verarbeitung haben, die deine Interessen oder Grundrechte und -freiheiten überwiegen, oder dass die Verarbeitung aus rechtlichen Gründen erforderlich ist. Weitere Informationen zu den Umständen, unter denen ein Widerspruch erfolgreich sein kann, findest du im Hilfebereich. Schutz deiner lebenswichtigen Interessen oder der einer anderen Person. Die verwendeten Informationskategorien, warum wir deine Informationen zum Schutz deiner lebenswichtigen Interessen oder der lebenswichtigen Interessen einer anderen Person verarbeiten, und wie die Verarbeitung erfolgt, werden im Folgenden aufgeführt. Schutz deiner lebenswichtigen Interessen und/oder der lebenswichtigen Interessen einer anderen Person: Wir verwenden automatische Verarbeitungstechniken, führen manuelle (menschliche) Überprüfungen durch und geben Informationen in Situationen, in denen die lebenswichtigen Interessen von jemandem Schutz bedürfen, z. B. in Notfällen, weiter, unter anderem an Strafverfolgungsbehörden und andere. Zu diesen lebenswichtigen Interessen zählen der Schutz des Lebens, der körperlichen und psychischen Gesundheit, des Wohlbefindens oder der Integrität von dir oder anderen sowie das Erkennen, Entfernen und Melden illegaler Inhalte. Durch den Schutz dieser lebenswichtigen Interessen möchten wir schädliches Verhalten bekämpfen und den Schutz, die Integrität und die Sicherheit fördern, beispielsweise wenn wir Meldungen über schädliches Verhalten nachgehen oder geeignete Maßnahmen ergreifen, wie die Weitergabe von Informationen an zuständige Behörden, wenn jemand Hilfe benötigt. Deine Aktivität und die von dir bereitgestellten Informationen: Inhalte, die du erstellst, wie Beiträge oder Kommentare oder Audio, Inhalte, die du über unsere Kamerafunktion oder deine Einstellungen für Aufnahmen oder über unsere sprachgestützten Funktionen bereitstellst, Nachrichten, die du sendest und empfängst, einschließlich ihrer Inhalte, vorbehaltlich des anwendbaren Rechts. Metadaten zu Inhalten und Nachrichten: Die Arten von Inhalten, die du dir ansiehst bzw. mit denen du interagierst. Die Apps und Funktionen, die du nutzt, und welche Handlungen du in ihnen durchführst. Käufe, die du tätigt, oder andere Transaktionen, die du durchführst, einschließlich gekürzter Kreditkartendaten. Hashtags, die du verwendest: Den Zeitpunkt, die Häufigkeit und die Dauer deiner Aktivitäten auf unseren Produkten. Freunde, Follower und andere Kontakte. App-, Browser- und Geräteinformationen: Geräteeigenschaften und Gerätesoftware. Was du gerade auf deinem Gerät tust (z. B. ob sich unsere App im Vordergrund befindet oder ob sich deine Maus bewegt), Identifikatoren, die dein Gerät von dem/den Gerät(en) anderer Nutzer unterscheiden, Gerätesignale, Informationen, die du über deine Geräteeinstellungen geteilt hast, Informationen zum Netzwerk, mit dem du dein Gerät verbindest, einschließlich deiner IP-Adresse. Informationen von Cookies und ähnlichen Technologien. Informationen von Partnern, Anbietern und Dritten. So fördern wir Schutz, Integrität und Sicherheit: Wir geben wir deine Informationen an Strafverfolgungsbehörden, Regierungsbehörden, Meta-Unternehmen, Dritte (einschließlich Branchenkollegen) und andere weiter, wenn wir in gutem Glauben davon ausgehen, dass dies notwendig ist, um eine Vielzahl von Situationen zu erkennen, zu verhindern und zu verfolgen, darunter: die unberechtigte Nutzung unserer Produkte. Ein Beispiel ansehen. Verstöße gegen unsere Nutzungsbedingungen und Richtlinien. Ein Beispiel ansehen. Verdächtige Aktivitäten untersuchen. Uns selbst schützen, einschließlich unserer Rechte, unseres Eigentums, unserer Mitarbeiter oder Produkte. Missbrauch, Betrug und andere schädliche oder illegale Aktivitäten in und außerhalb unserer Produkte verhindern, Dich und andere schützen, einschließlich im Rahmen einer Untersuchung oder behördlichen Anfrage, Notfallsituationen, wie zum Beispiel Lebensgefahr oder das Risiko einer drohenden Körperverletzung. Unberechtigte Nutzung unserer Produkte: Wenn du beispielsweise unrechtmäßig Daten von Facebook-Nutzern erhebst und nutzt, können wir deine Informationen weitergeben, um uns selbst gegen Klagen oder in Rechtsstreitigkeiten zu verteidigen. Verstöße gegen unsere Nutzungsbedingungen und Richtlinien: Wenn du zum Beispiel drohende oder gefährliche Inhalte veröffentlichst, können wir deine Informationen über die Meta-Unternehmen hinweg weitergeben, um uns selbst und andere zu schützen. Dies kann das Blockieren deines Zugriffs auf bestimmte Funktionen oder das Deaktivieren deines Kontos über die Meta-Unternehmen hinweg umfassen.

Datenschutzerklärung Signal (aktueller Stand, 25.5.2018)
Privacy Policy

Signal utilizes state-of-the-art security and end-to-end encryption to provide private messaging and Internet calling services to users worldwide ("Services"). Your calls and messages are always encrypted, so they can never be shared or viewed by anyone but yourself and the intended recipients. Information you provide: Account Information. You register a phone number when you create a Signal account. Phone numbers are used to provide our Services to you and other Signal users. You may optionally add other information to your account, such as a profile name and profile picture. This information is end-to-end encrypted. Messages: Signal cannot decrypt or otherwise access the content of your messages or calls. Signal queues end-to-end encrypted messages on its servers for delivery to devices that are temporarily offline (e.g. a phone whose battery has died). Your message history is stored on your own devices. Additional technical information is stored on our servers, including randomly generated authentication tokens, keys, push tokens, and other material that is necessary to establish calls and transmit messages. Signal limits this additional technical information to the minimum required to operate the Services.

Contacts. Signal can optionally discover which contacts in your address book are Signal users, using a service designed to protect the privacy of your contacts. Information from the contacts on your device may be cryptographically hashed and transmitted to the server in order to determine which of your contacts are registered. User Support: If you contact Signal User Support, any personal data you may share with us is kept only for the purposes of researching the issue and contacting you about your case. Managing your information: You can manage your personal information in Signal's application Settings. For example, you can update your profile information or choose to enable additional privacy features like a Registration Lock PIN. Information we may share: Third Parties. We work with third parties to provide some of our Services. For example, our Third-Party Providers send a verification code to your phone number when you register for our Services. These providers are bound by their Privacy Policies to safeguard that information. If you use other Third-Party Services like YouTube, Spotify, Giphy, etc. in connection with our Services, their Terms and Privacy Policies govern your use of those services. Other instances where Signal may need to share your data. To meet any applicable law, regulation, legal process or enforceable governmental request. To enforce applicable Terms, including investigation of potential violations. To detect, prevent, or otherwise address fraud, security, or technical issues.

To protect against harm to the rights, property, or safety of Signal, our users, or the public as required or permitted by law. Updates: We will update this privacy policy as needed so that it is current, accurate, and as clear as possible. Your continued use of our Services confirms your acceptance of our updated Privacy Policy. Terms: Please also read our Terms which also governs the terms of this Privacy Policy. Contact Us: If you have questions about our Privacy Policy please contact us at privacy@signal.org. Attn: Privacy Signal Messenger, LLC 650 Castro Street, Suite 120-223 Mountain View, CA 94041. Effective as of May 25, 2018.

Updated May 25, 2018

Datenrichtlinie Twitter

Bevor Sie scrollen, lesen Sie dies **Es ist wirklich schwer, alle mit einer Datenschutzerklärung zufrieden zu stellen. Die meisten Personen, die Twitter nutzen, wollen etwas Kurzes und leicht Verständliches.**

Wir wünschten zwar, wir könnten alles, was Sie wissen müssen, in einen Tweet packen, aber unsere Regulierungsbehörden verlangen von uns, dass wir unseren rechtlichen Verpflichtungen nachkommen und diese sehr detailliert beschreiben. Aus diesem Grund haben wir unsere Datenschutzerklärung so einfach wie möglich formuliert, um Sie in die Lage zu versetzen, informierte Entscheidungen zu treffen, wenn Sie Twitter nutzen, indem wir sicherstellen, dass Sie die von uns erhobenen Daten, wie sie verwendet werden und wann sie weitergegeben werden verstehen und darüber Kontrolle haben. Wenn Sie also nicht jedes Wort der Datenschutzerklärung lesen, sollten Sie wenigstens dies wissen: Twitter ist eine öffentliche Plattform. Erfahren Sie, was sichtbar und durchsuchbar ist. Wir erheben einige Daten über Sie. Erfahren Sie, was wir erheben und wie Dienste unserer verbundenen Unternehmen können ihre eigenen Erklärungen haben. Erfahren Sie mehr über verbundene Unternehmen. Wir verwenden Ihre Daten, um Twitter zu verbessern. Erfahren Sie, wie wir Ihre Daten nutzen. Sie können Ihr Erlebnis kontrollieren. Erfahren Sie, wie Sie Ihre Einstellungen aktualisieren können. Wenn Sie Fragen dazu haben, wie wir Daten nutzen, fragen Sie einfach. Erfahren Sie, wie Sie uns kontaktieren können.

Im Ernst – was passiert mit meinen Daten?

Welche Daten erheben Sie über mich? Sie geben Daten, wir bekommen Daten. Im Gegenzug bieten wir nützliche Dienste an. Nicht das, was Sie sich vorgestellt haben? Überprüfen Sie Ihre Einstellungen.

1. Daten, die wir erheben. Die **Daten, die wir erheben**, wenn Sie Twitter nutzen, **lassen sich in drei Kategorien unterteilen**. **1.1 Daten, die Sie uns zur Verfügung stellen**. Um einige unserer Produkte und Dienste nutzen zu können, benötigen Sie ein Konto und um ein Konto zu erstellen, müssen Sie uns bestimmte Daten zur Verfügung stellen. Wenn Sie ebenso unsere kostenpflichtigen Produkte und Dienste nutzen, können wir Ihnen diese nicht zur Verfügung stellen, ohne Zahlungsdaten zu erhalten. Grundsätzlich sind bestimmte Daten erforderlich, wenn Sie viele unserer Produkte und Dienste nutzen möchten. • **Persönliche Konten**. Wenn Sie ein Konto erstellen, müssen Sie uns einige Daten zur Verfügung stellen, damit wir Ihnen unsere Dienste anbieten können. Dazu gehören ein **Anzeigename** (zum Beispiel „Twitter Moments“); ein **Benutzername** (zum Beispiel @TwitterMoments); ein **Passwort**; eine **E-Mail-Adresse oder Telefonnummer**; ein **Geburtsdatum**, Ihre **Anzeigesprache** und **Daten zur einmaligen Anmeldung bei Dritten** (wenn Sie diese Anmeldemethode wählen). Sie können sich auch dafür entscheiden, Ihren **Standort in Ihrem Profil und in Ihren Tweets zu teilen** und Ihr **Adressbuch auf Twitter hochzuladen**, um die Suche nach Personen, die Sie kennen, zu erleichtern. Ihre **Profildaten, einschließlich Ihres Anzeigenamens und Ihres Benutzernamens, sind immer öffentlich**, aber Sie können entweder Ihren echten Namen oder ein Pseudonym verwenden. Denken Sie auch daran, dass Sie mehrere Twitter-Konten einrichten können, um zum Beispiel verschiedene Teile Ihrer Identität zum Ausdruck zu bringen, sei es beruflich oder anderweitig. • **Professionelle Konten**. Wenn Sie ein professionelles Konto einrichten, müssen Sie uns auch eine berufliche Kategorie angeben und können uns weitere Daten zur Verfügung stellen, einschließlich **Adresse, Kontakt-E-Mail-Adresse und Kontakt-Telefonnummer**, die alle immer öffentlich sind. • **Zahlungsdaten**. Um Werbeanzeigen oder andere Angebote zu kaufen, die als Teil unserer kostenpflichtigen Produkte und Dienste zur Verfügung gestellt werden, **müssen Sie uns Zahlungsdaten zur Verfügung stellen, einschließlich Ihrer Kredit- oder Debitkartennummer, des Ablaufdatums der Karte, des CVV-Codes und der Rechnungsadresse**. • **Präferenzen**. Wenn Sie Ihre Präferenzen über Ihre Einstellungen festlegen, erheben wir diese Daten, damit wir Ihre Präferenzen berücksichtigen können. **1.2 Daten, die wir erheben, wenn Sie Twitter nutzen**. Wenn Sie unsere Dienste nutzen, **erheben wir Daten darüber, wie Sie unsere Produkte und Dienste nutzen**. Wir verwenden diese Daten, um Ihnen Produkte und Dienste zur Verfügung zu stellen, um dabei zu helfen, Twitter sicherer und respektvoller für alle zu erhalten und um relevanter für Sie zu sein. **Daten über die Nutzung**. Wir **erheben Daten über Ihre Aktivitäten auf Twitter, einschließlich**: • **Tweets und anderer Inhalte, die Sie posten** (einschließlich des Datums, der Anwendung und der Version von Twitter) sowie Daten über Ihre **Broadcasting-Aktivitäten** (z. B. **TwitterLive oder Spaces**), einschließlich der von Ihnen erstellten **Broadcasts und des Zeitpunkts, zu dem Sie sie erstellt haben**, Ihrer **Listen, Lesezeichen und Communities, denen Sie zugehören**. • Ihre **Interaktionen mit den Inhalten anderer Nutzer**, wie z. B. **Retweets, Likes, Shares, Antworten, wenn andere Nutzer Sie in Inhalten erwähnen oder taggen oder wenn Sie sie erwähnen oder taggen und Broadcasts, an denen Sie teilgenommen haben** (einschließlich Ihres **Verlaufs der angesehenen Inhalte, des Zuhörens, Kommentierens, Sprechens und Reagierens**). • **Wie Sie mit anderen auf der Plattform interagieren**, beispielsweise mit **Personen, denen Sie folgen und Personen, die Ihnen folgen**, und wenn Sie **Direktnachrichten verwenden, einschließlich des Inhalts der Nachrichten, der Empfänger sowie Datum und Uhrzeit der Nachrichten**. • Wenn Sie mit uns kommunizieren,

beispielsweise per E-Mail, erheben wir Daten über die Kommunikation und deren Inhalt. • Wir erheben Daten über Links, mit denen Sie in unseren Diensten interagieren (auch in den E-Mails, die wir Ihnen schicken).. Käufe und Zahlungen. Um Ihnen zu ermöglichen, eine Zahlung zu tätigen oder Geld mithilfe von Twitter-Funktionen oder -Diensten zu senden, einschließlich über einen Zwischenhändler, können wir Daten über Ihre Transaktion erhalten, beispielsweise wann sie durchgeführt wurde, wann ein Abonnement abläuft oder sich automatisch verlängert und welche Beträge Sie gezahlt oder erhalten haben. Gerätedaten. Wir sammeln Daten von und über die Geräte, die Sie für den Zugriff auf Twitter nutzen, einschließlich: • Daten über Ihre Verbindung, wie beispielsweise Ihre IP-Adresse und den Browsertyp. • Daten über Ihr Gerät und deren Einstellungen, wie beispielsweise Geräte- und Werbe-ID, Betriebssystem, Anbieter, Sprache, Speicher, installierte Apps und Akkustand. • Das Adressbuch Ihres Geräts, wenn Sie sich dazu entschieden haben, es mit uns zu teilen. Standortdaten. Wenn Sie Twitter nutzen, erheben wir einige Daten über Ihren ungefähren Standort, um Ihnen den Dienst zu bieten, den Sie erwarten, einschließlich der Anzeige relevanter Werbeanzeigen. Sie können auch wählen, ob Sie Ihren aktuellen genauen Standort oder Orte, an denen Sie Twitter zuvor genutzt haben, teilen möchten, indem Sie diese Einstellungen in Ihrem Konto aktivieren. Vermutete Identität. Wir können Daten erheben oder erhalten, die wir verwenden, um Rückschlüsse auf Ihre Identität zu ziehen, wie unten beschrieben: • Wenn Sie sich mit einem Browser oder Gerät bei Twitter anmelden, werden wir diesen Browser oder dieses Gerät mit Ihrem Konto verknüpfen. Vorbehaltlich Ihrer Einstellungen können wir Ihr Konto auch mit anderen Browsern oder Geräten verknüpfen als mit denen, die Sie für die Anmeldung bei Twitter nutzen (oder Ihr abgemeldetes Gerät oder Ihren Browser mit anderen Browsern oder Geräten oder von Twitter generierten Identifikatoren verknüpfen). • Wenn Sie Twitter andere Daten zur Verfügung stellen, einschließlich einer E-Mail-Adresse oder Telefonnummer, verknüpfen wir diese Daten mit Ihrem Twitter-Konto. Vorbehaltlich Ihrer Einstellungen können wir diese Daten auch verwenden, um andere Daten über Ihre Identität abzuleiten, zum Beispiel indem wir Ihr Konto mit Hashes von E-Mail-Adressen verknüpfen, die gemeinsame Komponenten mit der E-Mail-Adresse haben, die Sie Twitter zur Verfügung gestellt haben. • Wenn Sie auf Twitter zugreifen und nicht angemeldet sind, können wir anhand der von uns erhobenen Daten Rückschlüsse auf Ihre Identität ziehen. Log-Daten. Wir können Daten erhalten, wenn Sie Inhalte auf unseren Produkten und Diensten ansehen oder anderweitig mit ihnen interagieren, auch wenn Sie kein Konto erstellt haben oder abgemeldet sind, wie beispielsweise: • IP-Adresse; Browsertyp und -sprache; Betriebssystem; die verweisende Webseite; Zugriffszeiten; besuchte Seiten; Standort; Ihr Mobilfunkanbieter; Gerätedaten (einschließlich Geräte- und Anwendungs-IDs); Suchbegriffe und -IDs (einschließlich derer, die nicht als Abfragen übermittelt wurden); Ihnen auf Twitter angezeigte Werbeanzeigen; von Twitter generierte Identifikatoren; und Identifikatoren, die mit Cookies verknüpft sind. Wir erhalten auch Log-Daten, wenn Sie auf Links in unseren Diensten klicken, diese ansehen oder mit ihnen interagieren, einschließlich wenn Sie eine andere Anwendung über Twitter installieren. Werbeanzeigen. Wenn Sie Anzeigen, die wir auf oder außerhalb von Twitter schalten, ansehen oder mit ihnen interagieren, können wir Daten über diese Ansichten oder Interaktionen erheben (z. B. das Ansehen einer Videoanzeige oder eines Prerolls, das Klicken auf eine Anzeige, die Interaktion mit Retweets oder Antworten auf eine Werbeanzeige). Cookies und ähnliche Technologien. Wie viele andere Websites verwenden wir Cookies und ähnliche Technologien, um zusätzliche Daten über die Nutzung der Website zu erheben und unsere Dienste zu betreiben. Für viele Bereiche unserer Produkte und Dienste, wie beispielsweise die Suche und das Ansehen öffentlicher Profile, sind Cookies nicht erforderlich. Hier können Sie mehr darüber erfahren, wie wir Cookies und ähnliche Technologien verwenden. Interaktionen mit unseren Inhalten auf Websites Dritter. Wenn Sie unsere Inhalte auf Websites von Dritten ansehen, die Twitter-Inhalte wie eingebettete Timelines oder Tweet-Buttons integrieren, können wir Log-Daten erhalten, einschließlich der von Ihnen besuchten Webseite. 1.3 Daten, die wir von Dritten erhalten. Wenn Sie andere Online-Produkte und -Dienste nutzen, können sie Daten über diese Nutzung an uns weitergeben. Werbepartner, Entwickler, Verleger. Unsere Werbe- und Geschäftspartner geben Daten wie Browser-Cookie-IDs, von Twitter generierte Identifikatoren, IDs von Mobilgeräten, gehashte Nutzerdaten wie E-Mail-Adressen, demografische Daten oder Interessensdaten sowie auf einer Website oder App angesehene Inhalte oder durchgeführte Aktionen an uns weiter. Einige unserer Werbepartner, insbesondere unsere Werbetreibenden, ermöglichen es uns auch, ähnliche Daten direkt von ihrer Website oder App zu erheben, indem sie unsere Werbetechnologie integrieren. Daten, die von Werbepartnern und verbundenen Unternehmen weitergegeben oder von Twitter von den Websites und Apps der Werbepartner und verbundenen Unternehmen erhoben werden, können mit den anderen Daten kombiniert werden, die Sie mit Twitter teilen und die Twitter erhält, generiert oder über Sie ableitet, wie an anderer Stelle in dieser Datenschutzerklärung beschrieben. Andere Dritte, Kontoverbindungen und Integrationen. Wir können Daten über Sie von Dritten erhalten, die nicht unsere Werbepartner sind, wie beispielsweise von anderen Twitter-Nutzern, Entwicklern und Partnern, die uns helfen, die Sicherheit und Qualität von Inhalten auf unserer Plattform zu bewerten, von unseren verbundenen

Unternehmen und von anderen Diensten, die Sie mit Ihrem Twitter-Konto verbinden. Sie können auswählen, Ihr Twitter-Konto mit Ihrem Konto bei einem anderen Dienst zu verbinden und dieser andere Dienst kann uns Daten über Ihr Konto bei diesem Dienst senden. Wie verwenden Sie meine Daten? Um Twitter zu dem Dienst zu machen, den Sie kennen und lieben.

2. Wie wir Daten verwenden

Aufgrund der Art und Weise, wie die Systeme funktionieren, die unsere Dienste für Sie anbieten, ist es nicht einfach, die Verwendung der von uns erhobenen Daten aufzuschlüsseln. So kann beispielsweise dieselbe Daten in verschiedener Art und Weise für verschiedene Zwecke verwendet werden, um letztlich einen einzigen Dienst zu erbringen. Wir halten es für am nützlichsten, die fünf wichtigsten Arten und Weisen, wie wir Daten verwenden, zu beschreiben. Wenn Sie Fragen haben, die nicht beantwortet werden, können Sie uns jederzeit kontaktieren. Los geht's:

2.1 Betreiben, Verbessern und Personalisieren unserer Dienste

Wir verwenden die von uns erhobenen Daten, um Twitter-Produkte und -Dienste anzubieten und zu betreiben. Wir verwenden die von uns erhobenen Daten auch, um unsere Produkte und Dienste zu verbessern und zu personalisieren, damit Sie ein besseres Erlebnis auf Twitter haben, einschließlich indem wir Ihnen relevantere Inhalte und Werbeanzeigen zeigen, Ihnen Personen und Themen vorschlagen, denen Sie folgen können und Ihnen helfen, verbundene Unternehmen, Apps von Dritten und Dienste zu entdecken. Wir können die Daten, die wir von Konten anderer Dienste erheben, bei denen Sie auswählen Ihr Twitter-Konto zu verbinden, verwenden, um Ihnen Funktionen wie dienstübergreifendes Posting oder dienstübergreifende Authentifizierung zu bieten und um unsere Dienste zu betreiben. Wir verwenden Ihre Kontaktdaten, um anderen zu helfen, Ihr Konto zu finden, wenn Ihre Einstellungen dies zulassen, einschließlich über Dienste von Dritten und Kundenanwendungen. **Wir verwenden Ihre Daten, um unsere Dienste für Werbung und gesponserte Inhalte vorbehaltlich Ihrer Einstellungen bereitzustellen, was dabei hilft, die Werbeanzeigen auf Twitter für Sie relevanter zu gestalten.** Wir verwenden diese Daten auch, um die Effektivität von Werbeanzeigen zu messen und um dabei zu helfen, Ihre Geräte zu erkennen, damit wir Ihnen Werbeanzeigen auf und außerhalb von Twitter anbieten können. Einige unserer Werbepartner ermöglichen es uns auch, ähnliche Daten direkt von ihrer Website oder App zu erheben, indem sie unsere Werbetechnologie integrieren. Daten, die von Werbepartnern und verbundenen Unternehmen weitergegeben oder von Twitter von den Websites und Apps von Werbepartnern und verbundenen Unternehmen erhoben werden, können mit den anderen Daten kombiniert werden, die Sie mit Twitter teilen und die Twitter erhält, generiert oder über Sie ableitet, wie an anderer Stelle in unserer Datenschutzerklärung beschrieben.

2.2 Förderung von Schutz und Sicherheit

Wir verwenden die von uns erhobenen Daten, um für den Schutz und die Sicherheit unserer Nutzer, unserer Produkte, Dienste und Ihres Kontos zu sorgen. Dazu gehören die Überprüfung Ihrer Identität, die Authentifizierung Ihres Kontos und die Abwehr von Betrug, unbefugter Nutzung und illegalen Aktivitäten. Wir verwenden die Daten auch, um die Sicherheit und Qualität der Inhalte auf Twitter zu bewerten und zu beeinflussen – dies beinhaltet die Untersuchung und Durchsetzung unserer Richtlinien und Bedingungen sowie des geltenden Rechts.

2.3 Messen, Analysieren und Verbessern unserer Dienste

Wir verwenden die von uns erhobenen Daten, um die Effektivität unserer Produkte und Dienste zu messen und zu analysieren und um besser zu verstehen, wie Sie sie nutzen, um sie zu verbessern.

2.4 Kommunikation mit Ihnen über unsere Dienste

Wir verwenden die von uns erhobenen Daten, um mit Ihnen über unsere Produkte und Dienste zu kommunizieren, einschließlich Produktaktualisierungen und Änderungen unserer Richtlinien und Bedingungen. Wenn Sie sich dafür entscheiden, können wir Ihnen auch gelegentlich Marketingnachrichten schicken.

2.5 Forschung

Wir verwenden Daten, die Sie mit uns teilen oder die wir erheben, um Forschung, Umfragen, Produkttests und Fehlerbehebungen durchzuführen, die uns helfen, unsere Produkte und Dienste zu betreiben und zu verbessern.

Meine Tweets sind öffentlich?!

Wie oder wann gibt Twitter meine Daten weiter?

Es gibt keine schnelle Antwort auf diese Frage, aber seien Sie gewarnt: Tweets können in den Nachrichten oder in einer Suchmaschine landen.

3. Weitergabe von Daten

Sie sollten wissen, auf welche Weise wir Ihre Daten weitergeben, warum wir sie weitergeben und wie Sie dies kontrollieren können. **Es gibt fünf grundsätzliche Möglichkeiten, wie wir Ihre Daten weitergeben.**

3.1 Wenn Sie tweeten, posten und teilen

Mit der breiten Öffentlichkeit. Sie weisen uns an, diese Daten so weit wie möglich offenzulegen. Die Inhalte von Twitter, einschließlich Ihrer Profildaten (z. B. Name/Pseudonym, Benutzername, Profilbilder), sind für die breite Öffentlichkeit zum Ansehen zugänglich. Die Öffentlichkeit muss sich nicht anmelden, um einen Großteil der Inhalte auf Twitter zu sehen. Sie können Twitter-Inhalte auch außerhalb von Twitter finden, zum Beispiel über die Ergebnisse von Suchanfragen in Internet-Suchmaschinen. Mit anderen Twitter-Nutzern. Abhängig von Ihren Einstellungen und basierend auf den Twitter-Produkten und -Diensten, die Sie nutzen, geben wir Folgendes weiter:

- Ihre Interaktionen mit Twitter-Inhalten anderer Nutzer, wie beispielsweise Likes und Personen, denen Sie folgen.
- Inhalte, die Sie an einen bestimmten Twitter-Nutzer senden, wie beispielsweise über Direktnachrichten.

Bitte bedenken Sie, dass, wenn Sie Daten wie Direktnachrichten oder geschützte Tweets mit jemandem geteilt haben, der über einen Dienst eines Dritten auf Twitter zugreift, die Daten an den Dienst des Dritten

weitergegeben werden können. Mit Partnern. Abhängig von Ihren Einstellungen stellen wir auch bestimmten Dritten Daten zur Verfügung, um uns beim Angebot oder Betrieb unserer Produkte und Dienste zu unterstützen. Sie können mehr über diese Partnerschaften in unserem Hilfe-Center erfahren. Sie können kontrollieren, ob Twitter Ihre personenbezogenen Daten an diese Partnern weitergibt, indem Sie die Option „Weitergabe von Daten an Geschäftspartner“ in Ihren Datenschutz- und Sicherheitseinstellungen verwenden. (Diese Einstellung steuert nicht die Weitergabe, die an anderer Stelle in dieser Datenschutzerklärung beschrieben wird, wie beispielsweise wenn wir Daten mit unseren Dienstleistern oder durch andere als die in diesem Hilfe-Center Artikel beschriebenen Partnerschaften teilen).

3.2 Mit Dritten & Integrationen von Dritten. Mit Dienstleistern. Wir können Ihre Daten an unsere Servicepartner weitergeben, die in unserem Auftrag Funktionen und Dienste erbringen, einschließlich Zahlungsdienstleister, die Zahlungen ermöglichen; Servicepartner, die unsere verschiedenen Blogs und Wikis hosten; Servicepartner, die uns helfen, die Nutzung unserer Dienste zu verstehen und solche, die Betrugserkennungsdienste anbieten. Mit Werbekunden. Werbeeinnahmen ermöglichen es uns, unsere Produkte und Dienste zur Verfügung zu stellen. Werbetreibende können Daten aus Ihrer Interaktion mit ihren Werbeanzeigen auf oder außerhalb von Twitter erhalten. Wenn Sie beispielsweise auf einen externen Link oder eine Werbeanzeige auf unseren Diensten klicken, kann der Werbetreibende oder der Betreiber der Website herausfinden, dass Sie von Twitter gekommen sind, zusammen mit anderen Daten, die mit der Werbeanzeige, auf die Sie geklickt haben, verknüpft sind, wie beispielsweise Merkmale des Publikums, das damit erreicht werden sollte, und andere von Twitter generierte Identifikatoren für diese Werbeanzeige. Sie können auch andere personenbezogene Daten von Ihnen erheben, wie beispielsweise Cookie-Identifikatoren oder Ihre IP-Adresse.

Inhalte und Integrationen von Dritten. Wir geben Ihre Daten mit Ihrer Einwilligung oder auf Ihre Anweisung hin weiter oder legen diese offen, beispielsweise wenn Sie einen Web-Client oder eine Anwendung eines Dritten autorisieren, auf Ihr Konto zuzugreifen oder wenn Sie uns anweisen, Ihr Feedback an ein Unternehmen weiterzugeben. Um gleichermaßen Ihr Erlebnis zu verbessern, arbeiten wir auch mit Dritten zusammen, um deren Videoinhalte auf Twitter anzuzeigen oder das plattformübergreifende Teilen zu ermöglichen. Wenn Sie sich Inhalte unserer Videopartner oder plattformübergreifenden Partner ansehen oder anderweitig mit diesen interagieren, können diese Ihre personenbezogene Daten erhalten und verarbeiten, wie in ihren Datenschutzerklärungen beschrieben. Bei Videoinhalten können Sie Ihre Autoplay-Einstellungen anpassen, wenn Sie es vorziehen, dass diese Inhalte nicht automatisch abgespielt werden. Durch unsere APIs. Wir verwenden Technologien wie APIs und Einbettungen, um öffentliche Twitter- Daten für Websites, Apps und andere zu ihrer Nutzung zur Verfügung zu stellen, zum Beispiel um Tweets auf einer Nachrichten-Website anzuzeigen oder zu analysieren, was Personen auf Twitter äußern. Wir stellen diese Inhalte in der Regel in begrenztem Umfang kostenlos zur Verfügung und erheben Lizenzgebühren für den Zugriff in großem Umfang. Wir haben Standardbedingungen, die regeln, wie diese Daten verwendet werden können und ein Compliance-Programm zur Durchsetzung dieser Bedingungen. Diese Personen und Unternehmen sind jedoch nicht mit Twitter verbunden und ihre Angebote spiegeln möglicherweise nicht die Aktualisierungen wider, die Sie auf Twitter vornehmen. Weitere Informationen darüber, wie wir öffentliche Daten über Twitter der Welt zur Verfügung stellen, finden Sie unter <https://developer.twitter.com>.

3.3 Wenn dies gesetzlich vorgeschrieben ist, um Schaden zu verhindern oder im öffentlichen Interesse. Wir können Ihre Daten aufbewahren, verwenden, weitergeben oder offenlegen, wenn wir glauben, dass dies vernünftigerweise notwendig ist, um:

- ein Gesetz oder eine Verordnung zu erfüllen oder einem Gerichtsverfahren oder einer behördlichen Aufforderung nachzukommen;
- die Sicherheit einer Person zu schützen, die Sicherheit oder Integrität unserer Plattform zu schützen, einschließlich, um die Verhinderung von Spam, Missbrauch oder böswilligen Akteuren auf unseren Diensten zu unterstützen;
- zu erklären, warum wir Inhalte oder Konten von unseren Diensten entfernt haben (z.B. wegen eines Verstoßes gegen die Twitter-Regeln);
- Betrugs-, Sicherheits- oder technische Probleme zu lösen; oder
- unsere Rechte oder unser Eigentum oder die Rechte oder das Eigentum derjenigen, die unsere Dienste nutzen, zu schützen.

3.4 Mit unseren verbundenen Unternehmen. Wir können Daten an unsere verbundenen Unternehmen weitergeben, um unsere Produkte und Dienste zur Verfügung zu stellen.

3.5 Als Folge einer Änderung der Eigentumsverhältnisse. Wir können Daten über Sie in Verbindung mit einer Fusion, Übernahme, Reorganisation, einem Verkauf von Vermögenswerten oder einem Konkurs weitergeben, verkaufen oder übertragen. Diese Datenschutzerklärung gilt für Ihre personenbezogenen Daten, die (vor und nach dem Abschluss einer Transaktion) an das neue Unternehmen weitergegeben oder übertragen werden. Haben Daten ein Verfallsdatum? Wie lange bewahren Sie die Daten auf? Grundsätzlich speichern wir Ihre Daten so lange, wie Ihr Konto aktiv ist.

4. Wie lange wir Daten aufbewahren Wir speichern verschiedene Arten von Daten für unterschiedliche Zeiträume:

- Wir speichern Ihre Profildaten und Inhalte für die Laufzeit Ihres Kontos.
- Andere personenbezogene Daten, die wir bei der Nutzung unserer Produkte und Dienste erheben, speichern wir in der Regel für eine Dauer von maximal 18 Monaten.
- Denken Sie daran, dass öffentliche Inhalte an anderer Stelle

existieren können, auch nachdem Sie sie von Twitter entfernt haben. Zum Beispiel können Suchmaschinen und andere Dritte Kopien Ihrer Beiträge länger aufbewahren, basierend auf ihren eigenen Datenschutzerklärungen, auch nachdem sie auf Twitter gelöscht wurden oder abgelaufen sind. Sie können hier mehr über die Auffindbarkeit in Suchen lesen. • Wenn Sie gegen unsere Regeln verstoßen und Ihr Konto gesperrt wird, können wir die Identifikatoren, die Sie zur Erstellung des Kontos verwendet haben (d.h. E-Mail-Adresse oder Telefonnummer), auf unbestimmte Zeit speichern, um zu verhindern, dass Wiederholungstäter neue Konten erstellen. • Es kann sein, dass wir bestimmte Daten länger aufbewahren, als in unseren Richtlinien festgelegt, um gesetzliche Anforderungen zu erfüllen und aus Gründen der Sicherheit. Wie kann ich meine Daten kontrollieren? Sie können auf sie zugreifen, sie löschen oder Ihre Einstellungen ändern. Im Grunde sind Sie der Chef. 5. Kontrolle übernehmen 5.1 Auskunft, Berichtigung, Übertragbarkeit. Sie können Auskunft über die Daten, die Sie uns zur Verfügung gestellt haben, verlangen, sie berichtigen oder ändern, indem Sie Ihr Profil bearbeiten und Ihre Kontoeinstellungen anpassen. • Sie können mehr über die Daten, die wir über Sie erhoben oder abgeleitet haben, unter Ihren Twitter-Daten erfahren und hier Auskunft über weitere Informationen verlangen. • Sie können eine Kopie Ihrer Daten, wie beispielsweise Ihre Tweets, herunterladen, indem Sie den Anweisungen hier folgen. • Auf der Website von Periscope können Sie die Berichtigung oder Änderung Ihrer Daten verlangen und Ihre Kontodaten herunterladen, indem Sie den Anweisungen hier folgen. Zum Schutz Ihrer Privatsphäre und zur Aufrechterhaltung der Sicherheit ergreifen wir Maßnahmen zur Überprüfung Ihrer Identität, bevor wir Ihnen Auskunft über Ihre personenbezogenen Daten gewähren oder einem Antrag auf Löschung, Übertragbarkeit oder einem anderen damit zusammenhängenden Antrag nachkommen. In bestimmten Situationen können wir Ihren Antrag auf Auskunft, Berichtigung oder Übertragbarkeit ablehnen, zum Beispiel wenn Sie Ihre Identität nicht nachweisen können. 5.2 Löschung Ihrer Daten. Wenn Sie den Anweisungen hier (oder für Periscope hier) folgen, wird Ihr Konto deaktiviert. Nach der Deaktivierung ist Ihr Twitter-Konto, einschließlich Ihres Anzeigenamens, Ihres Nutzernamens und Ihres öffentlichen Profils, nicht mehr auf Twitter.com, Twitter für iOS und Twitter für Android sichtbar. Für bis zu 30 Tage nach der Deaktivierung ist es immer noch möglich, Ihr Twitter-Konto wiederherzustellen, wenn es versehentlich oder fälschlicherweise deaktiviert wurde. 5.3 Widerspruch, Einschränkung oder Widerruf Ihrer Einwilligung. Hier können Sie Ihre Datenschutzeinstellungen und andere Kontofunktionen verwalten. Wenn Sie Ihre Einstellungen ändern, kann es einige Zeit dauern, bis Ihre Auswahl in unseren Systemen vollständig umgesetzt ist. Je nach den Einstellungen, die Sie angepasst haben, können Sie auch Änderungen in Ihrem Twitter-Erlebnis oder Einschränkungen beim Zugriff auf bestimmte Funktionen feststellen. Twitter hält sich an die Digital Advertising Alliance Self-Regulatory Principles for Online Behavioral Advertising (auch als „interessenbasierte Werbung“ bezeichnet) und respektiert das Consumer Choice Tool der DAA, mit dem Sie interessenbasierte Werbung unter <https://optout.aboutads.info/> ablehnen können. 5.4 Anfragen von bevollmächtigten Vertretern. Um eine Anfrage bezüglich der Auskunft, der Berichtigung oder der Löschung Ihrer Daten oder der Daten einer anderen Person, wenn Sie deren bevollmächtigter Vertreter sind, zu stellen, können Sie sich auch an uns wenden, wie im Abschnitt „Wie kann ich Twitter kontaktieren?“ unserer Datenschutzerklärung unten beschrieben. Wir können von Ihnen verlangen, dass Sie zusätzliche Daten zur Überprüfung zur Verfügung stellen. Wie geht Twitter mit meinen Daten um, egal wo ich bin? Wir behandeln Ihre Daten fair, unabhängig davon, wo auf der Welt Sie leben. 6. Ihre und unsere Rechte Wir stellen Twitter Personen auf der ganzen Welt zur Verfügung und bieten allen unseren Nutzern, unabhängig von ihrem Wohnort, viele der gleichen Datenschutz-Tools und Kontrollen. Es kann jedoch sein, dass Ihr Erlebnis etwas anders ist als das der Nutzer in anderen Ländern, um sicherzustellen, dass Twitter die lokalen Anforderungen respektiert. 6.1 Wir stützen uns auf bestimmte Rechtsgrundlagen für die Verwendung Ihrer Daten. Twitter hat sorgfältig die Rechtsgrundlagen geprüft, auf Grundlage dessen es Twitter erlaubt ist, Ihre Daten zu erheben, zu verwenden, weiterzugeben und anderweitig zu verarbeiten. Wenn Sie mehr erfahren und die Feinheiten besser verstehen möchten, empfehlen wir Ihnen, sich diese zusätzlichen Informationen über die Datenverarbeitung anzusehen. **Und nein, wir verkaufen Ihre personenbezogenen Daten nicht.** 6.2 Wir bewegen Ihre Daten, damit Twitter für Sie funktioniert. So wie Sie Twitter nutzen, um nahtlos an globalen Unterhaltungen mit Personen in Ländern auf der ganzen Welt teilzunehmen, muss Twitter Daten über Grenzen hinweg und in verschiedene Länder auf der ganzen Welt bewegen, um den sicheren und zuverlässigen Service zu unterstützen, auf den Sie sich verlassen. Wenn Sie zum Beispiel in Europa leben und ein Gespräch mit jemandem in den Vereinigten Staaten führen, müssen Daten zwischen diesen Ländern ausgetauscht werden, um diese Erfahrung zu ermöglichen – das ist es, was Sie von uns erwarten. Wir nutzen auch Rechenzentren und Cloud-Anbieter und beauftragen unsere verbundenen Unternehmen sowie Dritte und Servicepartner in vielen Teilen der Welt, um uns bei der Bereitstellung unserer Dienste zu unterstützen. Bevor wir Daten von einem Land in ein anderes bewegen, prüfen wir die Risiken, die sich für die Daten ergeben können, und stützen uns gegebenenfalls auf Instrumente wie **Standardvertragsklauseln**, um den Schutz Ihrer Betroffenenrechte zu gewährleisten. Wenn Daten an

Dritte weitergegeben werden, verlangen wir von diesen, dass sie den gleichen Schutz für Ihre Daten gewährleisten, den wir selbst bieten. Ist Twitter für Kinder geeignet? Nein, Twitter ist nicht für Personen unter 13 Jahren bestimmt. 7. Das Publikum von Twitter Unsere Dienste richten sich nicht an Kinder und Sie dürfen unsere Dienste nicht nutzen, wenn Sie unter 13 Jahre alt sind. Sie müssen außerdem alt genug sein, um in die Verarbeitung Ihrer personenbezogenen Daten in Ihrem Land einzuwilligen (in einigen Ländern können wir Ihrem Elternteil oder Erziehungsberechtigten erlauben, dies in Ihrem Namen zu tun). Bist du da, Twitter? Wird sich diese Erklärung ändern? Wenn sie sich ändern wird, werden wir es Ihnen mitteilen. 8. Änderungen an dieser Datenschutzerklärung Die aktuellste Version dieser Datenschutzerklärung regelt unsere Verarbeitung Ihrer personenbezogenen Daten und wir können diese Datenschutzerklärung gelegentlich nach Bedarf überarbeiten. Wenn wir diese Datenschutzerklärung überarbeiten und Änderungen vornehmen, die wir als wesentlich erachten, werden wir Sie darüber informieren und Ihnen die Möglichkeit geben, die überarbeitete Datenschutzerklärung zu überprüfen, bevor Sie Twitter weiter nutzen. Wie kann ich Twitter kontaktieren? Sliden Sie in unsere ... sehr offizielle Inbox. 9. Wie Sie Twitter kontaktieren können Wir möchten von Ihnen hören, wenn Sie Gedanken oder Fragen zu dieser Datenschutzerklärung haben. Sie können uns über unsere Seite für Anfragen zum Datenschutz kontaktieren oder uns an die unten angegebene Adresse schreiben. Wenn Sie in den Vereinigten Staaten oder einem anderen Land außerhalb der Europäischen Union, der EFTA-Staaten oder des Vereinigten Königreichs leben, ist der für Ihre personenbezogenen Daten Verantwortliche Twitter, Inc. mit der folgenden Adresse: Twitter, Inc. z.H.: Anfrage zur Datenschutzerklärung 1355 Market Street, Suite 900 San Francisco, CA 94103 Wenn Sie in der Europäischen Union, den EFTA-Staaten oder dem Vereinigten Königreich leben, ist der Verantwortliche Twitter International Unlimited Company mit der folgenden Adresse: Twitter International Unlimited Company z.H.: Datenschutzbeauftragter One Cumberland Place, Fenian Street Dublin 2, D02 AX07 IRELAND Sie können den Datenschutzbeauftragten von Twitter vertraulich über unser Datenschutz-Anfrageformular kontaktieren. Wenn Sie Bedenken bezüglich unserer Datenverarbeitungspraktiken äußern möchten, haben Sie das Recht, sich an Ihre örtliche Aufsichtsbehörde oder an die federführende Aufsichtsbehörde der Twitter International Unlimited Company, die Irish Data Protection Commission, zu wenden, indem Sie die auf ihrer Website aufgelisteten Kontaktdaten nutzen. Stand: 10. Juni 2022

Datenrichtlinie WhatsApp

Letzte Änderung: 14. November 2022 (archivierte Versionen)

WhatsApp Datenschutzrichtlinie

Inhaltsverzeichnis

Wichtige Updates

Rechtliche Hinweise zu WhatsApp

Informationen, die wir erheben

Informationen, die von dir und WhatsApp an Dritte weitergegeben werden

So arbeiten wir mit anderen Meta-Unternehmen zusammen

Wie und warum wir deine Informationen verarbeiten; unsere Rechtsgrundlagen für die Verarbeitung

So übst du deine Rechte aus

Aufbewahrung deiner Informationen

Löschen deiner Informationen

Verwaltung deiner Informationen

Zusammenarbeit mit Behörden, Beratern und Branchenpartnern

Übermittlung von Informationen in Länder außerhalb des EWR im Rahmen unserer globalen

Aktivitäten

Aktualisierungen unserer Datenschutzrichtlinie

Kontaktaufnahme mit uns: Wenn du nicht in der Europäischen Region lebst, stellt dir WhatsApp LLC die Dienste bereit und zwar gemäß diesen Nutzungsbedingungen und der Datenschutzrichtlinie.

Wichtige Updates: Wie bisher können wir deine privaten Nachrichten nicht lesen und auch bei deinen Anrufen nicht mithören, da beide Ende-zu-Ende-verschlüsselt sind. Daran wird sich nie etwas ändern.

Wir aktualisieren unsere Datenschutzrichtlinie, um zu erläutern, wie wir deine Daten schützen, wenn du bestimmte Funktionen auf WhatsApp nutzt: Wir haben unserer Beschreibung von Gruppen eine Erläuterung von Communitys hinzugefügt. Communitys ermöglichen es, zugehörige WhatsApp-Gruppen unter einem Dach zu organisieren. Das hilft Organisationen wie Nachbarschafts-Gruppen oder Universitätsvereinen, die Sicherheit ihrer Kommunikation zu gewährleisten und ihre Arbeit zu organisieren. Du kannst bestimmen, welchen Communitys du beitreten und welche du verlassen oder erstellen möchtest. Hier erfährst du mehr dazu. Wir haben Informationen zu Wearables und begleitenden Geräten (wie Smart-Brillen) hinzugefügt, die es dir ermöglichen, über die Geräte Nachrichten zu senden und Anrufe zu tätigen. Diese Funktion ist optional, und deine privaten Nachrichten und Sprachanrufe, die über Wearables und begleitende Geräte gesendet werden, sind immer Ende-zu-Ende-verschlüsselt. Hier erfährst du mehr dazu.

Wir haben eine Beschreibung von Avataren hinzugefügt. Avatare bieten eine neue Möglichkeit, dich darzustellen, ohne ein Foto zu verwenden, und können als Profilbild oder als individuelle Sticker in Chats genutzt werden. Das Erstellen eines Avatars ist optional, und du kannst bestimmen, wie du deinen Avatar nutzt. Hier erfährst du mehr dazu.

Wir haben weitere Informationen zur Suche nach Unternehmen auf WhatsApp hinzugefügt. Diese Funktion ist optional und macht es einfacher, nach Unternehmen zu suchen und einen Chat mit ihnen zu beginnen, ohne WhatsApp zu verlassen. Suchbegriffe werden in anonymisierter Form verarbeitet, sodass die Daten nicht mehr auf dein Konto zurückgeführt werden können. Hier erfährst du mehr dazu. Wir hoffen, du hast an der Verwendung von WhatsApp weiterhin Freude.

Rechtliche Hinweise zu WhatsApp: Wenn du in der Europäischen Region lebst, stellt dir WhatsApp Ireland Limited („WhatsApp“, „user/e/em/en/er/es“, „wir“ oder „uns“) unsere Dienste bereit und zwar gemäß den Nutzungsbedingungen und dieser Datenschutzrichtlinie. Wenn du außerhalb der Europäischen Region lebst, werden dir die Dienste von WhatsApp LLC bereitgestellt.

Der Respekt für deine Privatsphäre steht bei uns an erster Stelle. Seit dem Start von WhatsApp sind wir bestrebt, unsere Dienste unter Beachtung einer Reihe von strengen Datenschutzgrundsätzen aufzubauen. Wir sind eines der Meta-Unternehmen. In unserer Datenschutzrichtlinie („Datenschutzrichtlinie“) erläutern wir unsere Praktiken in Bezug auf Daten, insbesondere die Informationen, die wir zur Bereitstellung unserer Dienste verarbeiten.

So wird in der Datenschutzrichtlinie beispielsweise erklärt, welche Informationen wir erheben und welche Auswirkungen dies auf dich hat. Darin werden zudem die Maßnahmen beschrieben, die wir zum Schutz deiner Privatsphäre ergreifen, wie zum Beispiel, dass über unsere Dienste zugestellte Nachrichten nicht von uns gespeichert werden und dass wir dir die Kontrolle darüber geben, mit wem du auf unseren Diensten kommunizierst. Diese Datenschutzrichtlinie gilt für alle unsere Dienste, sofern nichts anderes angegeben wird. Bitte lies dir auch die WhatsApp Nutzungsbedingungen („Nutzungsbedingungen“, „Bedingungen“) durch, in denen die Bedingungen erläutert werden, gemäß denen du unsere Dienste nutzt und wir unsere Dienste bereitstellen.

Informationen, die wir erheben: **Die Arten von Informationen, die wir erhalten und erheben, hängen davon ab, wie du unsere Dienste nutzt.** Im Einklang mit unseren Bedingungen benötigen wir

bestimmte Konto-Informationen von dir, um unsere Dienste bereitstellen zu können, und wenn wir diese Informationen nicht haben, können wir dir unsere Dienste nicht bereitstellen. Beispielsweise musst du deine Mobiltelefonnummer angeben, wenn du ein Konto für die Nutzung unserer Dienste anlegen möchtest. Unsere Dienste verfügen über optionale Funktionen, für deren Bereitstellung – falls du sie nutzen möchtest – wir weitere Informationen erheben müssen. Du wirst gegebenenfalls über die Erhebung der jeweiligen Informationen informiert. Wenn du die Informationen, die zur Nutzung einer Funktion benötigt werden, nicht bereitstellen möchtest, kannst du die betreffende Funktion nicht nutzen. Beispiel: Du kannst deine genauen Standortinformationen nicht mit deinen Kontakten teilen, wenn du auf deinem Gerät nicht das Teilen des Standorts aktivierst. Berechtigungen kannst du in den gerätebasierten Einstellungen verwalten und zwar sowohl auf Android- als auch auf iOS-Geräten. Informationen, die du zur Verfügung stellst: Deine Konto-Informationen. Um ein WhatsApp-Konto zu erstellen, musst du deine Mobiltelefonnummer und einen Profilnamen deiner Wahl angeben. Wenn du uns diese Informationen nicht bereitstellst, kannst du kein Konto zur Nutzung unserer Dienste anlegen. Du kannst auch andere optionale Informationen zu deinem Konto hinzufügen, wie beispielsweise ein Profilbild und „Info“-Angaben. Benutzerinhalte. Deine Nachrichten, in Nachrichten enthaltene Medien und Anrufe: Wir bieten für unsere Dienste eine Ende-zu-Ende-Verschlüsselung an. Ende-zu-Ende-Verschlüsselung bedeutet, dass deine Anrufe, Nachrichten, in Nachrichten enthaltene Medien, darunter Inhalte wie Bilder, Audio, Video, Dokumente und Dateien, verschlüsselt sind, um sie davor zu schützen, dass Dritte (einschließlich WhatsApp) diese Inhalte sehen können. Erfahre mehr über Ende-zu-Ende-Verschlüsselung und darüber, wie Unternehmen auf WhatsApp mit dir kommunizieren. In der Regel werden deine Nachrichten auf deinem Gerät bzw. deinen Geräten gespeichert und nicht auf unseren Servern. Während der Zustellung speichern wir deine Nachrichten vorübergehend in verschlüsselter Form. Sobald deine Nachrichten zugestellt wurden, werden sie von unseren Servern gelöscht. Kann eine Nachricht nicht zugestellt werden, speichern wir sie bis zu 30 Tage in verschlüsselter Form auf unseren Servern und versuchen in dieser Zeit, sie zuzustellen. Wenn eine Nachricht nach 30 Tagen immer noch nicht zugestellt wurde, löschen wir sie. Wir können den Inhalt nicht zugestellter Nachrichten, die auf unseren Servern gespeichert sind, nicht sehen, da sie verschlüsselt sind. Wenn ein Benutzer in einer Nachricht Medien versendet, speichern wir diese Medien bis zu 30 Tage lang in verschlüsselter Form auf unseren Servern, um die Zustellung effizienter zu machen, etwa wenn Empfänger die Medien weiterleiten möchten. Wir können die Medien nicht sehen, da sie verschlüsselt sind. Status-Informationen. Du kannst entscheiden, ob du deinen Status teilen möchtest. Dieser wird ebenfalls Ende-zu-Ende-verschlüsselt. Genaue Standortinformationen. Wir versetzen dich in die Lage, genaue Standortinformationen von deinem Gerät zu teilen, wenn du standortbezogene Funktionen nutzt, z. B., wenn du deinen Standort mit deinen Kontakten teilst oder dir Standorte in der Nähe oder von deinen Kontakten mit dir geteilte Standorte ansiehst. Genaue Standortinformationen, die du in deinen Chats mit deinen Kontakten teilst, werden ebenfalls verschlüsselt, damit WhatsApp sie nicht sehen kann. Du kannst das Teilen deiner genauen Standortinformationen in deinen gerätebasierten Einstellungen in der App (weitere Informationen für iPhone und Android) sowie in deinen gerätebasierten Einstellungen steuern. Außerdem kannst du Inhalte bereitstellen, die nicht verschlüsselt werden. Das heißt, wir können sie sehen. Dazu gehören dein Profilbild, deine „Info“ sowie Namen und Beschreibungen deiner Communitys und Gruppen. Dein Netzwerk: Du kannst den Kontakt-Upload nutzen und uns regelmäßig die Telefonnummern im Adressbuch deines Geräts zur Verfügung stellen, darunter die Nummern von Benutzern unserer Dienste sowie die von deinen sonstigen Kontakten. Wenn einer deiner Kontakte unsere Dienste noch nicht benutzt, verwalten wir diese Information in einer Weise, die sicherstellen soll, dass diese Kontakte nicht von uns identifiziert werden können. Weitere Informationen zum Kontakt-Upload und den Informationen, die wir Personen zur Verfügung stellen, die WhatsApp nicht nutzen, findest du hier. Darüber hinaus erheben wir Informationen zu Benutzern, die dich kontaktieren und nicht in deinem Geräteadressbuch sind, sowie zu Benutzern, die du blockiert hast oder die dich blockiert haben. Deine Community- und Gruppeninformationen. Du kannst Communitys, Gruppen und Broadcast-Listen erstellen, ihnen beitreten oder zu ihnen hinzugefügt werden. Die jeweiligen Communitys, Gruppen und Listen werden dann mit deinem Konto verknüpft. Du gibst deinen Gruppen und Communitys einen Namen. Du kannst ein Community- oder Gruppenprofilbild oder eine entsprechende Beschreibung bereitstellen. Wir erheben außerdem Informationen darüber, wann Communitys und Gruppen erstellt oder aktualisiert werden. Informationen des Customer Supports und andere Mitteilungen. Wenn du uns für Zwecke des Customer Supports kontaktierst oder anderweitig mit uns kommunizierst, kannst du uns Informationen bezüglich deiner Nutzung unserer Dienste bereitstellen, etwa Kopien deiner Nachrichten, sonstige Informationen, die du als sachdienlich erachtest, damit wir deine Anfrage nachvollziehen und lösen können, sowie deine Kontaktinformationen (z. B. eine E-Mail-Adresse). Beispielsweise kannst du uns eine E-Mail mit Informationen zu Problemen mit der App-Leistung oder anderen Themen senden. Wir erheben zudem Informationen dazu, wie du unsere Customer Support-Funktionen nutzt (z. B. zu den Suchen, die du in

unserem Hilfebereich ausführst), sowie jegliches Feedback, das du uns zur Interaktion mit dem Customer Support gibst. Konto-Zugriffsinformationen: Wenn du dich bei unserem Dienst registrierst oder anmeldest, verifizieren wir deine **Telefonnummer**, indem wir dir per SMS einen Code senden oder dich anrufen. Du kannst auch eine PIN hinzufügen, um die Verifizierung in zwei Schritten zu aktivieren, und eine E-Mail-Adresse, die zum Zurücksetzen dieser PIN verwendet werden kann.

Automatisch erfasste Informationen: Nutzungsinformationen: **Wir erheben Informationen zu deiner Nutzung unserer Dienste.** Dies umfasst auch das Erheben von Informationen über deine Aktivität (beispielsweise wie du unsere Dienste nutzt), wie du mit anderen Benutzern unserer Dienste interagierst (z. B. wenn du nach einem Unternehmen suchst und mit ihm interagierst) sowie Zeitpunkt, Häufigkeit und Dauer deiner Aktivitäten. Dazu gehören auch Informationen zu den Funktionen, die du nutzt, z. B. unsere Nachrichtenfunktionen (und integrierte Anwendungen), Anruf-, Status-, Community-, Gruppen- oder Geschäftsfunktionen; ob du online bist; Zeitstempel für deine Nutzung, z. B. wann du unsere Dienste zuletzt genutzt hast (deine „Zuletzt online“-Angabe), und wann du Anrufe und Nachrichten tätigt bzw. sendest oder erhältst; und wann du zuletzt deine Profilinfo aktualisiert hast.

Protokoll- und Problemlösungsinformationen. Wir erheben Informationen darüber, wie gut unsere Dienste funktionieren, wenn du sie nutzt, darunter dienstspezifische Informationen für Diagnosezwecke und Performance-Informationen. Zu diesen Informationen gehören **Protokolldateien, Zeitstempel, Diagnose- oder Absturzdaten, Performance-Logs von Webseiten und Fehlerprotokolle oder Berichte.** Geräte- und Verbindungsdaten: Wenn du unsere Dienste installierst, nutzt oder auf sie zugreiffst, **erheben wir geräte- und verbindungs-spezifische Informationen.** Dazu gehören auch Informationen zu deinem Hardware-Modell und Betriebssystem, Batteriestand, Signalstärke, App-Version, Informationen zum Browser und Mobilfunknetz sowie zu der Verbindung, u. a. ob du WLAN oder mobile Daten nutzt, der Mobilfunk- oder Internetanbieter (ISP), Sprache und Zeitzone, IP-Adresse, Informationen zum Gerätebetrieb und Kennungen (einschließlich individueller IDs für Produkte von Meta-Unternehmen, die mit demselben Gerät oder Konto verknüpft sind).

Allgemeine Standortinformationen: Auch dann, wenn du unsere Funktionen im Zusammenhang mit deinem genauen Standort nicht nutzen möchtest (siehe Informationen, die von dir und WhatsApp an Dritte weitergegeben werden), **verwenden wir IP-Adressen und andere Informationen wie Telefonvorwahlen, um deinen ungefähren Standort zu bestimmen (z. B. das Land).**

Cookies: Um unsere webbasierten Dienste und die Webseite zu betreiben und zur Verfügung zu stellen, **erheben wir Informationen mithilfe von Cookies.** Erfahre mehr dazu, wie wir Cookies verwenden, um unsere Dienste zur Verfügung zu stellen. Benutzeroptionen: Wir erheben **Informationen über deine In-App-Einstellungen, Datenschutz-Einstellungen und Aufzeichnungen über die Annahme unserer Bedingungen** durch dich. Nur du hast die Kontrolle über deine Datenschutzeinstellungen. Damit kannst du ändern, wer deine „Zuletzt online“-Angaben, dein Profilbild, deine Profilinfo, Statusmeldungen, Lesebestätigungen sehen oder dich zu Gruppen hinzufügen kann. Wir erheben außerdem **Informationen dazu, ob du Push-Benachrichtigungen aktiviert hast und ob du selbstlöschende Nachrichten senden möchtest.** Authentifizierungsinformationen: Um dich bei Nutzung der Dienste zu verifizieren und dir die entsprechenden Genehmigungen zu erteilen (z. B. wenn du verschlüsselte Backups verwenden oder ein individuelles Passwort erstellen möchtest), **erstellen und speichern wir als Sicherheitsmaßnahme Authentifizierungscodes**, damit nur du auf dein Konto zugreifen kannst. Zu den Authentifizierungsinformationen gehören auch deine öffentlichen Verschlüsselungsschlüssel, die unser Ende-zu-Ende-Verschlüsselungsprotokoll verwendet. Nachrichten werden verschlüsselt, bevor sie bei unseren Servern ankommen. Das heißt, wir können sie nicht sehen. Von Dritten über dich bereitgestellte Informationen: Von anderen über dich bereitgestellte Informationen. **Wir erhalten Informationen über dich von anderen Benutzern.** Wenn beispielsweise andere Benutzer, die du kennst, unsere Dienste nutzen, stellen sie unter Umständen **deine Telefonnummer zur Verfügung**, wenn sie den Kontakt-Upload nutzen, so wie auch du ihre Telefonnummer bereitstellen kannst. Wir verlangen von allen diesen Benutzern, dass sie dazu berechtigt sind, deine Informationen zu erheben, zu verwenden und zu teilen, bevor sie uns irgendwelche Informationen bereitstellen. Sie können auch Nachrichten an dich oder an Gruppen senden, denen du angehörst, oder dich anrufen. Du solltest dir immer bewusst sein, dass generell jeder beliebige Benutzer Screenshots von deinen Chats oder Nachrichten machen oder Telefongespräche zwischen dir und ihm aufzeichnen und an WhatsApp oder irgendwelche anderen Personen senden oder auf anderen Plattformen veröffentlichen kann. Meldungen von Benutzern: So wie du andere Benutzer melden kannst, können auch andere Benutzer oder Dritte deine Interaktionen und Nachrichten zwischen dir und ihnen oder anderen auf unseren Diensten an uns melden; beispielsweise, um mögliche Verstöße gegen unsere Bedingungen oder Richtlinien zu melden. Wenn über die entsprechenden Tools eine Meldung an uns gesendet wird, erhalten wir von der meldenden Person Informationen sowohl zu dem meldenden Benutzer als auch zu den von der Meldung betroffenen Personen. Mehr über die Informationen, die wir im Rahmen von Meldungen von Benutzern erhalten, und über den Umgang mit einer solchen Meldung erfährst du unter Informationen

zum Blockieren und Melden von Kontakten. Unternehmen auf WhatsApp: Wenn Unternehmen, mit denen du während der Nutzung unserer Dienste interagierst, uns Informationen über ihre Interaktionen mit dir zur Verfügung stellen, verpflichten wir jedes dieser Unternehmen, im Einklang mit dem anwendbaren Recht zu handeln. Wenn du auf WhatsApp Nachrichten mit einem Unternehmen austauschst, solltest du dir bewusst sein, dass der Inhalt dieser Nachrichten für mehrere Personen in diesem Unternehmen sichtbar sein kann. Außerdem arbeiten manche Unternehmen mit Drittdienstleistern zusammen (wozu auch Meta gehören kann), die sie bei der Kommunikation mit ihren Kunden unterstützen. Beispielsweise könnte ein Unternehmen solchen Drittdienstleistern Zugriff auf seine Mitteilungen gewähren, damit diese sie versenden, speichern, lesen, verwalten oder anderweitig für das Unternehmen verarbeiten können. Damit du weißt, wie ein Unternehmen deine Informationen verarbeitet (und zum Beispiel deine Informationen an Dritte oder Meta weitergibt), solltest du dir die Datenschutzrichtlinie dieses Unternehmens durchlesen oder dich direkt an dieses Unternehmen wenden. Dienste Dritter: WhatsApp erhält Informationen über Übeltäter und Missbrauch von Meta-Unternehmen sowie App-Verifizierungsinformationen von Missbrauchsbekämpfungsdiensten, um die Sicherheit und Integrität zu fördern. Wenn Meta beispielsweise von einer Betrugsmethode erfährt, die Personen dazu auffordert, per WhatsApp eine Telefonnummer zu kontaktieren, gibt Meta diese Telefonnummer unter Umständen an WhatsApp weiter, damit wir das WhatsApp-Konto überprüfen können. Wir gestatten dir auch, unsere Dienste in Verbindung mit Diensten Dritter und mit Produkten von Meta-Unternehmen zu nutzen. Wenn du unsere Dienste mit solchen Diensten Dritter oder mit Produkten von Meta-Unternehmen nutzt, erhalten wir von diesen möglicherweise Informationen über dich; zum Beispiel, wenn du den „Teilen“-Button von WhatsApp in einem Nachrichtendienst nutzt, um einen Nachrichtenartikel mit deinen WhatsApp Kontakten oder den Gruppen bzw. Broadcast-Listen auf unseren Diensten zu teilen. Bitte beachte, dass bei deiner Nutzung von Diensten Dritter oder von Produkten von Meta-Unternehmen für deine Nutzung solcher Dienste und Produkte die Bedingungen und Datenschutzrichtlinien des Unternehmens gelten, das diese Dienste anbietet. Informationen, die von dir und WhatsApp an Dritte weitergegeben werden: Du teilst deine Informationen, wenn du unsere Dienste nutzt und über sie kommunizierst, und wir teilen deine Informationen, damit wir unsere Dienste betreiben, anbieten, verbessern, verstehen, individualisieren und unterstützen können. Sende deine Informationen an die Personen, mit denen du dich entscheidest zu kommunizieren. Du teilst Benutzerinhalte, wenn du über unsere Dienste kommunizierst. Du hast die Kontrolle darüber, was du beim Senden deiner Informationen an die WhatsApp-Benutzer (Einzelpersonen oder Unternehmen), mit denen du kommunizierst, übermittelst. Bedenke hierbei, dass WhatsApp-Benutzer Benutzerinhalte in unseren Diensten und außerhalb davon speichern und erneut mit anderen teilen können, sobald du sie gesendet hast. Mit deinem Konto verknüpfte Informationen. Im Rahmen deines WhatsApp-Chat-Erlebnisses und basierend auf deinen Datenschutz-Einstellungen können die Benutzer, die deine Telefonnummer in ihrem Gerät gespeichert haben, deine Konto-Informationen sehen (Telefonnummer, Profilbild, Profilinfo) und dich zu Gruppen und Communitys hinzufügen. Dort sind diese Informationen möglicherweise für andere Mitglieder der Gruppe oder Community sichtbar. Wenn du eine Nachricht an einen anderen Benutzer oder eine Gruppe sendest, wird dein ausgewählter Profilname für die Empfänger der Nachricht sichtbar, darunter auch Benutzer, bei denen du nicht in der Kontaktliste gespeichert bist. Je nach deinen Datenschutz-Einstellungen können Benutzer, die deine Telefonnummer in ihrem Gerät gespeichert haben, auch deine „Zuletzt online“-Angabe und deine Nachrichtenempfangsbestätigungen sehen. Du kannst deine Datenschutz-Einstellungen anpassen, um die Mitgliedschaft in Gruppen zu verwalten und festzulegen, ob bestimmte Informationen (z. B. „Zuletzt online“) für andere Benutzer verfügbar sind. In unserem Hilfebereich erfährst du mehr zum Thema Datenschutz-Einstellungen anpassen. Dienste Dritter. Wenn du oder andere Benutzer, mit denen du interagierst, Dienste Dritter oder andere Produkte von Meta-Unternehmen in Anspruch nimmst, auf die über unsere Dienste zugegriffen werden kann, erhalten die Anbieter dieser Dienste oder Produkte unter Umständen die Informationen über dich, die du oder andere mit ihnen teilen. Beispiele: Wenn du einen in unsere Dienste integrierten Datensicherungsdienst (wie iCloud oder Google Drive) nutzt, so erhält dieser die Informationen, die du mit ihm teilst, z. B. deine WhatsApp-Nachrichten. Wenn du über WhatsApp im Internet nach einem Gruppenprofilbild suchst, erhält der Anbieter der Suchmaschine den von dir verwendeten Suchbegriff. Wenn du über unsere Dienste mit einem Dienst Dritter oder anderen Produkten von Meta-Unternehmen interagierst, z. B. wenn du den In-App-Player zur Wiedergabe von Inhalten von einer Drittplattform wie YouTube oder Facebook nutzt, werden dem Anbieter des Dienstes bzw. der Produkte möglicherweise Informationen wie deine IP-Adresse und technische Informationen zur Verfügung gestellt, die zeigen, dass die Anfrage von einer WhatsApp-App stammt. Bitte beachte, dass bei deiner Nutzung von Drittanbieterdiensten oder von anderen Produkten von Meta-Unternehmen deren eigene Bedingungen und Datenschutzrichtlinien für deine Nutzung dieser Dienste und Produkte gelten. Drittdienstleister. Wir arbeiten mit Drittdienstleistern zusammen, die uns bei der Bereitstellung unserer Dienste unterstützen. Wenn wir

Informationen mit in dieser Funktion agierenden Drittdienstleistern teilen, verlangen wir von ihnen, dass sie deine Informationen in unserem Auftrag gemäß unseren Anweisungen und Bedingungen verwenden. Wir arbeiten mit den folgenden Arten von Drittdienstleistern zusammen: Anbietern von Telekommunikationstechnologie, damit wir dir zur Verifizierung deines Kontos SMS-Nachrichten senden oder dich anrufen können. Damit wir diese Dienste bereitstellen können, erhalten diese Anbieter deine Konto-Informationen (Telefonnummer) sowie Konto-Zugriffsinformationen (Verifizierungs-codes, damit du eine neue Telefonnummer oder ein neues Gerät, die bzw. das mit deinem Konto verbunden ist, verifizieren kannst). Die Anbieter, mit denen wir derzeit zusammenarbeiten, haben ihren Sitz in Schweden, den Niederlanden, dem Vereinigten Königreich und den Vereinigten Staaten. Einem Dienstleister für Inhaltssicherheitstechnologie, der uns dabei unterstützt, die Sicherheit und Integrität der Dienste durch Erkennung und Priorisierung von schädlichem Material für die Prüfung durch unsere Reviewer zu gewährleisten. Zur Erbringung dieser Dienstleistungen erhält dieser Anbieter bestimmte Bilder aus Meldungen von Benutzern (z. B. Bilder), aus „Deine Konto-Informationen“ (z. B. ein Profilbild) und aus „Deine Community- und Gruppeninformationen“ (z. B. ein Community- oder Gruppenprofilbild). Der Anbieter, mit dem wir derzeit zusammenarbeiten, hat seinen Sitz in den Vereinigten Staaten. Einem Standortdatenanbieter, damit du deinen Standort oder einen Ort in der Nähe mit anderen WhatsApp-Benutzern teilen kannst. Zur Erbringung dieser Dienstleistungen erhält dieser Anbieter genaue Standortinformationen (deinen aktuellen Standort und andere Standorte, die du auf der Karte auswählst). Der Anbieter, mit dem wir derzeit zusammenarbeiten, hat seinen Sitz in den Vereinigten Staaten. Welche sonstigen Informationen wir teilen, erfährst du in den Abschnitten So arbeitet WhatsApp mit anderen Meta-Unternehmen zusammen und Zusammenarbeit mit Behörden, Beratern und Branchenpartnern. So arbeiten wir mit anderen Meta-Unternehmen zusammen: WhatsApp ist eines der Meta-Unternehmen. Die Meta-Unternehmen stellen Personen und Unternehmen Technologieprodukte und dienstleistungen zur Verfügung. Wir arbeiten mit anderen Meta-Unternehmen zusammen, die als unsere Dienstleister fungieren und uns bei der Bereitstellung und Verbesserung unserer Dienste unterstützen. Wenn Meta-Unternehmen als unsere Dienstleister fungieren, verlangen wir von ihnen, dass sie deine Informationen in unserem Auftrag gemäß unseren Anweisungen und Bedingungen verwenden. Wir arbeiten mit Meta-Unternehmen in den Vereinigten Staaten und in Irland zusammen, die uns beim Betrieb unserer Dienste unterstützen. Damit wir diese Dienstleistungen erhalten, teilen wir Informationen, die wir erheben. Wir arbeiten mit Meta-Unternehmen sowie anderen im Eigentum von Meta befindlichen Unternehmen in den Vereinigten Staaten und Spanien zusammen, die Datenhosting- und Infrastruktur-Dienstleistungen bereitstellen, darunter die Verwendung von Rechenzentren zusammen mit den zugehörigen Dienstleistungen und Geräten, die für den Betrieb der Dienste erforderlich sind. Wir geben die Informationen, die wir erheben, an diese Unternehmen weiter. Wir arbeiten mit Meta-Unternehmen im Vereinigten Königreich, Israel und den Vereinigten Staaten zusammen, die uns Geschäftsanalyse-Dienstleistungen zur Verfügung stellen, damit wir beispielsweise ermitteln können, wie viele einzigartige Benutzer wir im Vergleich zu anderen Diensten haben, die angeboten werden von den Meta-Unternehmen. Wir teilen Deine Konto-Informationen (Telefonnummer), Geräte- und Verbindungsdaten (IDs, die mit demselben Gerät oder Konto verbunden sind, Hardwaremodell, Betriebssysteminformationen und App-Versionen, Ländervorwahl und Netzwerkcode), Benutzeroptionen (Aufzeichnungen über die Annahme von Bedingungen und Benutzereinstellungen) und Nutzungsinformationen (wann du WhatsApp zum letzten Mal benutzt hast und das Datum, an dem du dein Konto zum ersten Mal registriert hast, Zeit der Aktivitäten). Wir arbeiten mit einem Meta-Unternehmen in den Vereinigten Staaten zusammen, das Dienstleistungen für folgende Zwecke bereitstellt: Unterstützung bei der Durchführung der zweistufigen Authentifizierung und Bereitstellung von technischer Unterstützung und Problemlösung in Bezug auf unsere Interaktion mit Mobilfunknetzen. Wir teilen deine Konto-Informationen (Telefonnummer) und Konto-Zugriffsinformationen (Verifizierungscode), um diese Dienstleistung zu erhalten. Wir arbeiten mit anderen Meta-Unternehmen: in den Vereinigten Staaten und Spanien zusammen, die uns betriebliche, administrative und Customer Support-Dienstleistungen für folgende Zwecke bereitstellen: Betrieb, Verbesserung und Entwicklung der Dienste; Entwicklung, Korrektur und Anpassung der Dienste; Beantwortung der Anfragen von Benutzern/Nicht-Nutzern sowie Support im Zusammenhang mit den Anfragen; Schutz und Sicherheit der Konten; Vertragsverwaltung, Projektmanagement, Planung und verwandte Zwecke; und Durchführung von Umfragen zur Kundenzufriedenheit. im Vereinigten Königreich, den Vereinigten Staaten und Spanien zusammen, die folgende Dienstleistungen für uns erbringen: Produktrecherchen und -tests für (Funktionen von) Dienstleistungen, damit wir unsere Dienste verbessern können; und Fehlerbehebung von technischen Problemen und Sicherstellung des reibungslosen Betriebs der Dienste. im Vereinigten Königreich, Irland, Spanien, Deutschland und den Vereinigten Staaten zusammen, die uns Rechtsberatung und juristische Unterstützungsleistungen für folgende Zwecke bereitstellen: Gerichtsverfahren und andere Streitverfahren; Ermittlungen von Aufsichtsbehörden und andere gesetzliche Verfahren; Bearbeitung

von Beschwerden und/oder Anfragen von betroffenen Personen; Bearbeitung von behördlichen und anderen rechtlichen Anfragen; unsere rechtlichen Verwaltungsangelegenheiten; Management von datenschutzbezogenen Anfragen, darunter Entwicklung von Tools und Aufzeichnungsspeichern; und sonstige juristische Unterstützung, die gelegentlich angefordert wird. in den Vereinigten Staaten und Singapur zusammen, die uns bei der Bearbeitung rechtlicher und behördlicher Anfragen gemäß den anwendbaren Gesetzen und Vorschriften unterstützen, darunter auch in Notfallsituationen: Offenlegung relevanter personenbezogener Daten gegenüber Strafverfolgungs-, Regierungs-, Aufsichtsbehörden oder anderen; und Offenlegung personenbezogener Daten gegenüber Dritten im Zusammenhang mit zivilrechtlichen Verfahren. in den Vereinigten Staaten, dem Vereinigten Königreich und Spanien zusammen, die Verwaltungsdienstleistungen bereitstellen, damit wir durch folgende Maßnahmen besser für den Schutz und die Sicherheit der Dienste sorgen können: Untersuchung von verdächtigen Aktivitäten oder Verstößen gegen unsere Richtlinien; und Entfernen von Konten, die gegen unsere Richtlinien verstoßen. in Irland, den Vereinigten Staaten und Singapur zusammen, die uns Dienstleistungen zum Schutz vor Verletzungen unseres geistigen Eigentums durch folgende Maßnahmen zur Verfügung stellen: Prüfung von Konten auf Verstöße gegen WhatsApp-Richtlinien; Unterstützung bei Durchsetzungsmaßnahmen gegen diese Konten; Bereitstellung regelmäßiger Berichte an uns zu einzelnen Konten, die geprüft wurden und gegen die Durchsetzungsmaßnahmen ergriffen wurden; und Eskalation von Fällen, die juristisch geprüft werden müssen, an uns. Als Voraussetzung für den Erhalt der oben aufgeführten Dienstleistungen und je nach Dienstleistung, die erbracht wird, geben wir die Informationen, die wir erheben weiter. Wenn du mehr über die Meta-Unternehmen erfahren möchtest, die derzeit als Dienstleister für uns tätig sind, klicke bitte hier. Wie und warum wir deine Informationen verarbeiten; unsere Rechtsgrundlagen für die Verarbeitung: Nach geltendem Datenschutzrecht in der Europäischen Region (wie der DSGVO) müssen Unternehmen über eine Rechtsgrundlage für die Verarbeitung von Informationen verfügen. Wir stützen uns bei der Verarbeitung deiner Informationen zu den diversen in dieser Datenschutzrichtlinie beschriebenen Zwecken auf verschiedene Rechtsgrundlagen. Für jede nachstehend aufgeführte Rechtsgrundlage beschreiben wir die Zwecke der Verarbeitung (den Grund, warum wir deine Informationen verarbeiten) sowie unsere Verarbeitungsaktivitäten (die Art und Weise, auf die wir deine Informationen verarbeiten). Zudem listen wir die Kategorien deiner Informationen auf, die wir zu jedem einzelnen Zweck verarbeiten. Je nachdem, welche Rechtsgrundlage wir nutzen, stehen dir außerdem bestimmte Rechte zu, die wir im Folgenden erläutern. Du solltest wissen, dass dir ungeachtet der geltenden Rechtsgrundlage immer das Recht auf Auskunftserteilung, Berichtigung und Löschung deiner Informationen zusteht. Im Abschnitt So übst du deine Rechte aus findest du entsprechende Informationen, wenn du eines der Rechte in Anspruch nehmen möchtest. Informationen, die wir verarbeiten, um deine Nachrichten oder Anrufe zu übermitteln (darunter Informationen wie deine Telefonnummer, Datum und Uhrzeit eines Anrufs oder einer Nachricht oder Dauer deiner Anrufe), unterliegen den jeweiligen Regeln und Anforderungen der EU-Richtlinie 2002/58/EG und werden entsprechend gehandhabt, sofern diese anwendbar ist. Verarbeitung erforderlich zur Erfüllung unseres Vertrags mit dir Wir verarbeiten Informationen, wie es für den Abschluss und die Erfüllung unseres Vertrags mit dir, unserer Bedingungen, erforderlich ist. Die Kategorien der verwendeten Daten sowie die Gründe und Art ihrer Verarbeitung sind unten aufgeführt: Warum wir deine Informationen verarbeiten / Verwendete Kategorien von Informationen: Damit wir unsere Dienste wie im Abschnitt der Bedingungen „Unsere Dienste“ beschrieben betreiben, bereitstellen, verbessern, anpassen und unterstützen können – dies umfasst die Bereitstellung von Möglichkeiten für dich, dich mit anderen WhatsApp-Benutzern (einschließlich Unternehmen) zu verbinden und mit ihnen zu kommunizieren –, leistet WhatsApp Folgendes: Warum: Unterstützung beim Erstellen und Verwalten deines WhatsApp-Kontos durch: Erfassen und Verifizieren deiner Telefonnummer, indem wir dir einen Verifizierungscode per SMS senden oder dich anrufen. Prüfen des Betriebssystems und anderer Funktionen deines Geräts, um WhatsApp korrekt auf deinem Gerät einrichten zu können, und Ausführen von Sicherheitsprüfungen, um sicherzustellen, dass du nicht bereits ein Konto oder eine Telefonnummer besitzt, die für WhatsApp gesperrt sind. Aufzeichnen deiner Benutzereinstellungen, einschließlich der von dir angenommenen Bedingungen, deiner Datenschutz-Einstellungen und der von dir blockierten Benutzer. Ermöglichen, zusätzliche Informationen wie den von dir erstellten Avatar oder Konto-Informationen wie ein Profilbild oder Informationen über dich hinzuzufügen, die Personen, die deine Telefonnummer haben, entsprechend deinen Datenschutz-Einstellungen angezeigt werden. Ändern der Telefonnummer, die mit deinem WhatsApp-Konto verknüpft ist, wenn du diese aktualisierst. Zur Aufrechterhaltung der Sicherheit, Begrenzung der Datenspeicherung und zum Schutz deiner Privatsphäre, prüfen wir alle 30 Tage, ob eine Aktivität vorliegt und löschen dein Konto in der Regel, wenn dein Telefon 120 Tage lang nicht online war. Weitere Informationen erhältst du hier in unserem Hilfebereich. Löschen deines Kontos auf deine Anforderung hin (Informationen zum Löschen deines Kontos auf deinem iPhone und zum Löschen deines Kontos auf deinem Android-Gerät) oder entsprechend unseren Bedingungen. Wir

können dein Konto sperren, wenn du unsere Bedingungen, beispielsweise die Regelungen zur zulässigen Nutzung unserer Dienste, verletzt. Ermöglichen, dass du dein Konto erneut registrierst, wenn es deaktiviert oder gesperrt wurde. Kategorien: **Deine Konto-Informationen, Dein Netzwerk, Konto-Zugriffsinformationen, Nutzungsinformationen, Protokoll- und Problemlösungsinformationen, Geräte- und Verbindungsdaten, Allgemeine Standortinformationen, Benutzeroptionen, Authentifizierungsinformationen.** Warum: Ermöglichung der Verwendung und Verwaltung deines WhatsApp-Kontos auf verschiedenen Geräten durch: Verknüpfen eines neuen Geräts mit deinem Konto, damit du WhatsApp auf weiteren Geräten nutzen kannst und wir bestimmte weitere Geräte auf unseren Servern registrieren können. Synchronisieren deiner Konto-Informationen und Benutzeroptionen über deine Geräte hinweg mittels einer Aktualisierung, die an andere mit deinem Konto verknüpfte Geräte gesendet wird. Senden einer Ende-zu-Ende-verschlüsselten Kopie deines Chatverlaufs an deine neuen verknüpften Geräte, wenn du deine Chats synchronisierst (wir speichern diese verschlüsselte Kopie vorübergehend, um die Synchronisierung abzuschließen). Kategorien: Zum Verknüpfen eines Geräts mit deinem Konto: **Deine Konto-Informationen, Geräte- und Verbindungsdaten, Authentifizierungsinformationen, Nutzungsinformationen, Protokoll- und Problemlösungsinformationen, Zum Synchronisieren deiner Konto-Informationen und Benutzeroptionen zwischen deinen Geräten: Deine Konto-Informationen, Protokoll- und Problemlösungsinformationen, Geräte- und Verbindungsdaten, Benutzeroptionen** Zum Synchronisieren deines Chatverlaufs zwischen deinen Geräten: **Deine Konto-Informationen, Benutzerinhalte (deine Nachrichten, Bilder, Audiodateien und Videos sind Ende-zu-Ende-verschlüsselt), Protokoll- und Problemlösungsinformationen, Geräte- und Verbindungsdaten, Authentifizierungsinformationen.** Warum: Zum Senden und Empfangen Ende-zu-Ende-verschlüsselter Nachrichten und zum Übermitteln deines Status tun wir Folgendes: Wir ermöglichen dir, auf Nachrichten zu antworten, sie weiterzuleiten und zu löschen oder andere Arten von Nachrichten zu senden, etwa Sprachnachrichten, Nachrichten zur Einmalansicht oder selbstlöschende Nachrichten. Wenn das Gerät des Empfängers mit WhatsApp verbunden ist, senden wir Nachrichten direkt an dieses Gerät. Wenn dein Gerät oder das Gerät des Empfängers offline ist, speichern wir die verschlüsselte Nachricht bis zu 30 Tage lang, während wir versuchen, die Nachricht zu übermitteln, und senden eine Push-Benachrichtigung an das Gerät. Wir zeigen Empfängern in einem Chat an, wenn du online bist, oder geben deine Aktivität an, beispielsweise können Empfänger entsprechend deinen Benutzeroptionen sehen, wann du zuletzt online warst. Wir ermöglichen dir, das Internet nach Bildern zu durchsuchen, die du als Community- oder Gruppenprofilbild verwenden kannst, oder Videos von Drittanbieterdiensten wie YouTube zu teilen. Ist der entsprechende Link ein Video, zeigen wir eine Vorschau an und ermöglichen dem Empfänger, sich das Video im Chat anzusehen. Wir ermöglichen dir, deine Statusmeldung an Kontakte deiner Wahl zu senden. Statusmeldungen verschwinden nach 24 Stunden. Wir ergreifen Maßnahmen, um sicherzustellen, dass deine Nachrichten korrekt übertragen werden. Wir optimieren das Senden von Mediendateien, indem wir sie vorübergehend bis zu 30 Tage lang verschlüsselt auf unseren Servern speichern, um eine effizientere Übermittlung zu fördern. Wir geben dir und Dritten (wie Unternehmen) die Möglichkeit, über unsere Dienste miteinander zu kommunizieren und zu interagieren; dazu gehören z. B. Kataloge für Unternehmen auf WhatsApp, in denen du nach Produkten und Dienstleistungen suchst und Bestellungen aufgeben kannst. Wir nutzen Cookies, um unsere webbasierten Dienste zu betreiben und bereitzustellen. Kategorien: Zum Senden und Empfangen Ende-zu-Ende-verschlüsselter Nachrichten und zum Übermitteln deines Status: **Deine Konto-Informationen, Benutzerinhalte (deine Nachrichten, Bilder, Audiodateien, Videos, Dokumente und Dateien werden genau wie der von dir geteilte Status Ende-zu-Ende-verschlüsselt), Dein Netzwerk, Deine Community- und Gruppeninformationen, Protokoll- und Problemlösungsinformationen, Geräte- und Verbindungsdaten, Cookies, Benutzeroptionen, Authentifizierungsinformationen.** Zum Anzeigen deiner Anwesenheit (in Chats mit Einzelpersonen) und wann du zuletzt online warst: **Dein Netzwerk, Nutzungsinformationen (Online- oder Offline-Status), Benutzeroptionen.** Zum Anzeigen deiner Aktivitätsindikatoren: **Dein Netzwerk, Deine Community- und Gruppeninformationen, Nutzungsinformationen (ob du gerade schreibst oder nicht schreibst oder eine Sprachnachricht aufnimmst).** Zum Teilen deines Status: **Benutzerinhalte (Status wird Ende-zu-Ende-verschlüsselt), Dein Netzwerk, Benutzeroptionen** Warum: Zum allgemeinen Betreiben, Bereitstellen und Verbessern unserer Dienste tun wir Folgendes: Analysieren von Protokollinformationen, um Abstürze und Benutzerprobleme zu beheben. Erfassen von Informationen für Problembeseitigung, Diagnose und Fehlersuche. Erfassen und Erstellen von Metriken (wie Nachrichtenvolumen und Latenzen), um die Performance, Zuverlässigkeit und Effizienz von Diensten zu überwachen, damit wir die Dienstqualität sicherstellen und optimieren können. Testen unserer neuen Funktionen, um zu sehen, ob sie funktionieren, Durchführen von Versuchen, um die Wirkung neuer Funktionen zu bewerten, und Nachverfolgen von Übernahmemetriken (z. B. Prozentsatz der Benutzer, die ihren Status aktualisieren). Erfassen und

Erstellen von Aktivitäts- und Systemereignissen, um grob, z. B. auf Landes- oder App-Versionsebene, zu verstehen, wie und wie oft der Dienst genutzt wird.

Kategorien: Zum allgemeinen Betreiben, Bereitstellen und Verbessern unserer Dienste:

Deine Konto-Informationen, Deine Community- und Gruppeninformationen, Nutzungsinformationen, Protokoll- und Problemlösungsinformationen, Geräte- und Verbindungsdaten, Allgemeine

Standortinformationen: Warum: Damit du dich mit Unternehmen verbinden kannst, tun wir Folgendes: Wir ermöglichen dir, auf dem Dienst nach Unternehmen zu suchen bzw. sie zu entdecken.

Kategorien: Damit du dich mit Unternehmen verbinden kannst: Nutzungsinformationen, Protokoll- und Problemlösungsinformationen, Geräte- und Verbindungsdaten, Allgemeine Standortinformationen, Authentifizierungsinformationen: Warum: Zum Tätigen, Empfangen oder Verlassen von bzw. Beitreten zu Sprach- und Videoanrufen tun wir Folgendes: Erstellen einer Ende-zu-Ende-verschlüsselten Verbindung für Audio-/Videoinformationen zwischen dir und dem anderen Anrufteilnehmer (oder Teilnehmern, falls es sich um einen Gruppenanruf handelt), nachdem die Datenschutz-Einstellungen des Teilnehmers geprüft wurden, um sicherzustellen, dass du nicht blockiert wurdest.

Senden einer Push-Benachrichtigung an dich, wenn du einen Anruf erhältst oder verpasst hast.

Benachrichtigen von Teilnehmern in einem Gruppenanruf, wenn: ein anderer Benutzer eingeladen wurde, den Anruf aber nicht angenommen hat, ein anderer Benutzer anruft, ein anderer Benutzer dem Anruf beiträgt, ein Anrufteilnehmer aufgelegt hat und der Anruf beendet ist. Wenn du deine In-App-Einstellungen änderst oder bestimmte Aktionen in einem Anruf ausführst, lassen wir den bzw. die anderen Anrufteilnehmer wissen: ob dein Video ein- oder ausgeschaltet ist; wenn du andere Benutzer einlädst, von einem Audio- zu einem Videoanruf zu wechseln (oder andersherum); wenn du nichts von den anderen Anrufteilnehmern gehört hast; wenn du die Stummschaltung aktivierst oder deaktivierst; wenn deine Akkuladung unter 5 % beträgt und das Gerät nicht aufgeladen wird; wenn du einen Anruf erhältst, der deinen laufenden Anruf in WhatsApp unterbricht. Zum Optimieren der Anrufqualität tun wir Folgendes: Wechseln zu alternativen Netzwerkschnittstellen, wenn deine bestehende Verbindung eingeschränkt ist, und Erfassen erstellter Anrufmetriken (nur für iOS). Nachverfolgen von Metriken wie fehlgeschlagene Anrufe, Anzahl von Anrufen, die aufgrund einer Verbindungstrennung beendet wurden, und Messen der Netzwerkverbindungsbedingungen, um Probleme mit der Anrufqualität zu identifizieren und zu beheben. Speichern von Performance-Informationen auf deinem Gerät nach Anrufen, damit sich einfacher ein erneuter Anruf mit den gleichen Benutzern tätigen lässt.

Erfassen und Erstellen von Metriken über Anrufe, um die Anrufqualität zu optimieren.

Sichern deines Datenverbrauchs und der in einem Anruf verbrachten Zeit. **Austauschen von Netzwerk- und anderen Informationen** während eines Anrufs, um Audio-, Video- und Netzwerkqualität anzupassen. Kategorien: Zum Tätigen, Empfangen oder Verlassen von bzw. Beitreten zu Sprach- und Videoanrufen tun wir Folgendes: **Deine Konto-Informationen, Benutzerinhalte, Dein Netzwerk, Deine Community- und Gruppeninformationen, Protokoll- und Problemlösungsinformationen, Geräte- und Verbindungsdaten, Allgemeine Standortinformationen, Benutzeroptionen,**

Authentifizierungsinformationen: Zum Benachrichtigen der Anrufteilnehmer über Änderungen während eines Anrufs: Geräte- und Verbindungsdaten. Zum Optimieren der Anrufqualität: **Protokoll- und Problemlösungsinformationen, Geräte- und Verbindungsdaten.** Warum: Um dir zu helfen zu ermitteln,

ob deine Kontakte WhatsApp-Benutzer sind, wenn du das Adressbuch deines Geräts über den Kontakt-Upload synchronisieren möchtest, tun wir Folgendes: Regelmäßiges Identifizieren anderer WhatsApp-Benutzer in deinem Adressbuch, Hinzufügen dieser zu deiner WhatsApp-Kontaktliste und Speichern kryptografischer Hashwerte der Telefonnummern der Kontakte, die keine WhatsApp-Benutzer sind, damit wir deine WhatsApp-Kontakte schnell aktualisieren können, wenn sich diese Kontakte zu einem späteren Zeitpunkt bei WhatsApp registrieren. Hier erfährst du mehr dazu.

Entfernen von Kontakten aus deiner WhatsApp-Kontaktliste, wenn einer deiner Kontakte kein Konto mehr besitzt. Auf deine Anfrage hin Blockieren von Telefonnummern anderer Benutzer, um zu verhindern, dass sie dich in WhatsApp kontaktieren können. Zum Ermöglichen der Nutzung von Kontakt-Upload: Deine Konto-Informationen, Dein Netzwerk, Protokoll- und

Problemlösungsinformationen, Benutzeroptionen. Warum: Um dir zu ermöglichen, Communitys und Gruppen zu erstellen, ihnen beizutreten, sie zu verlassen und dich in ihnen zu vernetzen, um gleichzeitig mit mehreren Kontakten zu kommunizieren, tun wir Folgendes:

Prüfen, ob die Besitzer der Telefonnummer, die du einer Gruppe hinzufügen möchtest, WhatsApp-Benutzer sind, und sicherstellen, dass deren Aufnahme in die Gruppe ihren Datenschutz-Einstellungen entspricht. Sicherstellen, dass der Community- oder Gruppenname und die optionale Community- oder Gruppenbeschreibung den WhatsApp-Anforderungen entsprechen.

Speichern von Informationen zu der Community oder Gruppe und ihren Teilnehmern (einschließlich ausstehender oder früherer Teilnehmer), um sicherzustellen, dass die entsprechenden Berechtigungen angewendet werden, und Zuweisen des Erstellers der Community oder Gruppe als Admin, damit er die Infos, Mitglieder und Einstellungen der Community oder Gruppe steuern und personalisieren kann. Bei aktiven Communitys oder Gruppen protokollieren, wenn du Einladungen an

neue Community- oder Gruppenteilnehmer sendest, und für Gruppen Einladungen löschen, die innerhalb eines festgelegten Zeitraums nicht angenommen werden. Benachrichtigen der Teilnehmer der Gruppe über bestimmte wichtige Änderungen an der Community oder Gruppe, etwa Änderungen des Namens, der Beschreibung oder des Profilbilds der Community oder Gruppe, oder wenn eine Nachricht gelöscht wird. Vorübergehendes Speichern von Informationen, um zu verhindern, dass du Gruppen, die du verlassen hast, wieder hinzugefügt wirst, und Speichern von Telefonnummern von Teilnehmern, die beispielsweise aus Gruppen gesperrt wurden, damit sie diesen nicht wieder beitreten können. Diese Informationen werden auch verwendet, um verdächtige Benutzer oder missbräuchliches Verhalten zu identifizieren, wenn Teilnehmer schnell wechseln. Dir das Ernennen anderer Community-Admins für eine Community, die du erstellt hast oder von der du ein Community-Admin bist, und das Ernennen eines neuen Gruppenadmins oder Community-Admins gestatten, wenn aktuelle Admins die Gruppe oder Community verlassen oder ihr Konto löschen. Löschen einer Gruppe, wenn das letzte Mitglied die Gruppe verlässt. Aussetzen oder Deaktivieren einer Community und Hinzufügen oder Abtrennen von Gruppen in der Community. Zum Erstellen einer Gruppe oder Community: Deine Konto-Informationen, Dein Netzwerk, Deine Community- und Gruppeninformationen, Protokoll- und Problemlösungsinformationen, Benutzeroptionen, Authentifizierungsinformationen. Zum Verwalten aktiver Gruppen oder Communitys: Deine Konto-Informationen, Dein Netzwerk, Deine Community- und Gruppeninformationen, Protokoll- und Problemlösungsinformationen, Benutzeroptionen, Authentifizierungsinformationen Unterstützung beim Erstellen von Backups deines Chatverlaufs (und der Medien im Chatverlauf), wenn du dies anforderst, durch: Ermöglichen, ein Backup deines Chatverlaufs in einen cloudbasierten Drittanbieterdienst (wie Google Drive oder iCloud) hochzuladen. Ende-zu-Ende-Verschlüsseln deines Chatverlaufs mit einem zufällig generierten Verschlüsselungsschlüssel oder einem von dir erstellten Passwort. Du kannst diese verschlüsselten Backups deines Chatverlaufs in einen cloudbasierten Drittanbieterdienst (wie Google Drive oder iCloud) hochladen. Verwenden eines Verschlüsselungsschlüssels oder deines Passworts, um einen Verschlüsselungsschlüssel für die Entschlüsselung deines gesicherten Chatverlaufs abzurufen. Zum Erstellen, Aufrufen und Wiederherstellen von Backups und verschlüsselten Backups: Deine Konto-Informationen, Authentifizierungsinformationen (zum Authentifizieren eines Verschlüsselungsschlüssels oder Passworts). Zum Schutz der Sicherheit und Integrität unserer Dienste. Wir verwenden Informationen in unserem Besitz, wenden automatisierte Datenverarbeitungstechniken an und führen in einigen Fällen manuelle Prüfungen durch Menschen durch, um Folgendes zu tun: Laufendes Verifizieren und Prüfen, dass Benutzeranmeldungen echt sind. Protokollieren von Ereignissen und aggregierten Zahlen über Community-, Gruppen- und Benutzeraktionen im Hinblick auf unsere Dienste (etwa die Anzahl der Gruppen, denen du beigetreten bist) und zugehörige Sequenzen, wie Muster bei der Registrierung und wiederholte oder identische Meldungen von Benutzern, um verdächtige Benutzer, missbräuchliches Verhalten oder die Nutzung einer falschen WhatsApp-App oder einer Imitation unserer Dienste zu identifizieren und zu untersuchen. Untersuchen und Adressieren von Verletzungen unserer Bedingungen. Beispielsweise können wir dein Konto sperren, wenn wir erfahren, dass du an Verstößen beteiligt bist. Ermitteln, Verhindern und Bekämpfen schädlicher oder unrechtmäßiger Verhaltensweisen, etwa das Bekämpfen von Scraping durch Übeltäter, das Erkennen und Verhindern von Spam und negativen Erlebnissen. Erfassen von App-Verifizierungsinformationen von Missbrauchsabwehrdiensten, um unsere integritätsbezogenen Maßnahmen zu unterstützen. Zum Schutz der Sicherheit und Integrität unserer Dienste: Deine Konto-Informationen, Benutzerinhalte (sofern von einem Benutzer bereitgestellt), Dein Netzwerk, Deine Community- und Gruppeninformationen, Informationen des Customer Supports und andere Mitteilungen, Konto-Zugriffsinformationen, Nutzungsinformationen, Protokoll- und Problemlösungsinformationen, Geräte- und Verbindungsdaten, Allgemeine Standortinformationen, Cookies, Benutzeroptionen, Authentifizierungsinformationen, Von anderen über dich bereitgestellte Informationen, Meldungen von Benutzern, Unternehmen auf WhatsApp, Dienste Dritter. Übertragen, Speichern oder Verarbeiten deiner Informationen außerhalb des Europäischen Wirtschaftsraums. Da der WhatsApp-Service global betrieben wird und Benutzer und Unternehmen auf der ganzen Welt umfasst, müssen wir die von uns erfassten Informationen weltweit weitergeben, sowohl intern innerhalb der Meta-Unternehmen und dorthin, wo sich unsere Rechenzentren befinden, als auch extern an unsere Drittdienstleister. Wir nehmen notwendige Übermittlungen außerhalb des Europäischen Wirtschaftsraums vor, unter anderem in die Vereinigten Staaten und in andere Länder, um Folgendes tun zu können: Betreiben und Bereitstellen unserer Dienste. Außerdem ermöglichen wir dir, Informationen an deine Familie und deine Freunde auf der ganzen Welt weiterzugeben und mit ihnen in Kontakt zu treten und Korrigieren, Analysieren und Verbessern unserer Dienste. Weitere Informationen hierzu erhältst du im nachstehenden Abschnitt Übermittlung von Informationen in Länder außerhalb des EWR im Rahmen unserer globalen Aktivitäten. Zum Betreiben und Bereitstellen unserer Dienste: Deine Konto-Informationen, Benutzerinhalte, Dein Netzwerk, Deine Community- und Gruppeninformationen,

Informationen des Customer Supports und andere Mitteilungen, Konto-Zugriffsinformationen, Nutzungsinformationen, Protokoll- und Problemlösungsinformationen, Geräte- und Verbindungsdaten, Allgemeine Standortinformationen, Cookies, Benutzeroptionen, Authentifizierungsinformationen, Von anderen über dich bereitgestellte Informationen, Meldungen von Benutzern, Unternehmen auf WhatsApp, Dienste Dritter. Um mit dir über dienstbezogene Themen zu kommunizieren, tun wir Folgendes: Identifizieren relevanter dienstbezogener Benachrichtigungen für dich, Versenden dieser Benachrichtigungen an dich in WhatsApp und Protokollieren, wann du die Benachrichtigung erhalten hast. Werden beispielsweise unsere Bedingungen aktualisiert, senden wir eine Benachrichtigung über das Update. Zum Versenden von Benachrichtigungen oder Updates über unsere Dienste an dich: Deine Konto-Informationen, Protokoll- und Problemlösungsinformationen (Details der Benachrichtigungen, die du zuvor erhalten hast), Geräte- und Verbindungsdaten, Allgemeine Standortinformationen. Bereitstellen von Customer Support durch: Verarbeiten von Anforderungen im Hinblick auf Support und/oder Suchen, die du im WhatsApp-Hilfebereich, in der App oder über die WhatsApp-Website vornimmst. Antworten, wenn du unsere Hilfe anforderst, etwa Hilfe bei der Anmeldung bei deinem Konto oder beim Verifizierungsprozess. Zum Bereitstellen von Customer Support: Deine Konto-Informationen, Dein Netzwerk, Deine Community- und Gruppeninformationen, Informationen des Customer Supports und andere Mitteilungen, Konto-Zugriffsinformationen, Nutzungsinformationen, Protokoll- und Problemlösungsinformationen, Geräte- und Verbindungsdaten, Allgemeine Standortinformationen, Cookies. Wenn wir Informationen, die du uns bereitstellst, in dem für die Erfüllung unserer Vertragsbeziehung mit dir erforderlichen Maß verarbeiten, hast du entsprechend der anwendbaren Datenschutzgesetze das Recht auf Datenübertragbarkeit. Wenn du deine Rechte ausüben möchtest, lies bitte den Abschnitt So übst du deine Rechte aus dieser Datenschutzrichtlinie. Die anderen Rechtsgrundlagen, auf die wir uns bei der Verarbeitung deiner Informationen stützen, und die Umstände, unter denen wir uns auf sie stützen, sind unten aufgeführt: Deine Einwilligung: Wir verarbeiten Informationen zu den unten beschriebenen Zwecken, wenn du uns deine Einwilligung gegeben hast, um bestimmte Produktfunktionen in deinen gerätebasierten Einstellungen zu aktivieren. Die Kategorien der verwendeten Informationen sowie die Gründe und Art ihrer Verarbeitung sind unten aufgeführt: Zum Erfassen von Informationen über die von dir aktivierten gerätebasierten Einstellungen, zum Beispiel: Teilen der genauen Standortinformationen deines Geräts, wenn du unsere standortbezogenen Funktionen verwenden möchtest. Du kannst deinen aktuellen Standort mit deinen Kontakten teilen oder ihnen deinen Live-Standort senden oder einen Ort in deiner Nähe auf deiner Karte ansehen. Wenn dein Live-Standort geteilt wird, siehst du in der Live-Standort-Option in deinen Datenschutz-Einstellungen, in welchen Chats dein Live-Standort geteilt wird. Genaue Standortinformationen, die du in deinen Chats teilst, werden Ende-zu-Ende-verschlüsselt, das heißt WhatsApp kann sie nicht sehen. Zugreifen auf deine Kamera und/oder Fotogalerie, wenn du Fotos oder Medien mit deinen WhatsApp-Kontakten teilen möchtest. Fotos und Medien, die du in deinen persönlichen Chats teilst, sind Ende-zu-Ende-verschlüsselt.

Kategorien: Benutzerinhalte. Wenn wir deine Informationen auf Grundlage deiner Einwilligung verarbeiten, hast du das Recht, diese Einwilligung jederzeit zu widerrufen; dies berührt dann allerdings nicht die Rechtmäßigkeit der auf Grundlage deiner Einwilligung erfolgenden Verarbeitung vor deinem Widerruf. Wenn du deine Rechte ausüben möchtest, öffne bitte deine gerätebasierten Einstellungen oder deine In-App-Einstellungen (wie deine Live-Standort-Option) oder lies den Abschnitt So übst du deine Rechte aus dieser Datenschutzrichtlinie. Erfüllung einer rechtlichen Verpflichtung Wir verarbeiten Informationen, um eine rechtliche Verpflichtung zu erfüllen, darunter u. a. das Aufrufen, Aufbewahren oder Offenlegen bestimmter Informationen im Fall einer berechtigten rechtlichen Anfrage. Beispiele für irische und EU-Gesetze, die eine rechtliche Verpflichtung begründen könnten, die uns zur Verarbeitung von Informationen verpflichtet, sind unten aufgeführt. Im Hinblick auf unsere Verarbeitung können neue Gesetze erlassen oder andere Verpflichtungen verbindlich werden. Deshalb werden wir die Liste der Gesetze regelmäßig aktualisieren. Zur Verarbeitung von Informationen, wenn wir eine rechtliche Verpflichtung erfüllen, darunter u. a. das Aufrufen, Aufbewahren oder Offenlegen bestimmter Informationen, im Fall einer berechtigten rechtlichen Anfrage von einer Aufsichts-, Strafverfolgungs- oder anderen Behörde. Beispielsweise aufgrund eines Durchsuchungsbefehls oder einer Aufforderung zur Vorlage seitens einer irischen Strafverfolgungsbehörde zur Bereitstellung von Informationen im Zusammenhang mit einer Untersuchung, etwa deines Profilbildes oder deiner IP-Adresse. Beispiele für irische und EU-Gesetze, die in Irland durchsetzbar sind und eine Verpflichtung begründen könnten, aufgrund derer wir Informationen zu deiner Person verarbeiten müssen, sind etwa die folgenden: Zivil- und Handelssachen: Wenn uns ein Gerichtsbeschluss vorgelegt wird, aufgrund dessen wir Informationen für ein Gerichtsverfahren offenlegen müssen, etwa gemäß Verordnung (EU) Nr. 1215/2012 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen. Strafsachen: Um Anfragen von irischen Strafverfolgungsbehörden im Hinblick auf die Bereitstellung von Daten im Zusammenhang mit einer Untersuchung zu erfüllen, etwa gemäß

Paragraf 10 des Criminal Justice (Miscellaneous Provisions) Act 1997, geändert durch 6(1)(a) des Criminal Justice Act 2006, oder im Hinblick auf die Einleitung von Schritten zur Meldung von Informationen an Strafverfolgungsbehörden, falls erforderlich. Verbrauchersachen: Zur Erfüllung von Verpflichtungen gemäß dem Verbraucherrecht, etwa dem Competition and Consumer Protection Act 2014, zum Beispiel wenn die irische Wettbewerbs- und Verbraucherschutzkommission Informationen anfordert. Unternehmens- und Steuersachen: Zur Erfüllung unserer Verpflichtungen gemäß der Unternehmensgesetzgebung und dem Steuerrecht, etwa dem Companies Act 2014, sofern die irische Steuerbehörde Informationen anfordert. Aufsichtsrechtliche Angelegenheiten: Zur Erfüllung unserer Verpflichtungen im Hinblick auf die Zusammenarbeit mit Aufsichtsbehörden, etwa der irischen Data Protection Commission gemäß der Datenschutz-Grundverordnung und dem Data Protection Act 2018. Hier findest du die aktuelle Liste der Gesetze, die in Irland durchsetzbar sind und eine rechtliche Verpflichtung für WhatsApp begründen, die zu der Verarbeitung von Informationen führt. Im Hinblick auf unsere Verarbeitung deiner Informationen können neue Gesetze erlassen und andere Verpflichtungen verbindlich werden, wodurch wir verpflichtet werden können, deine Informationen zu verarbeiten. Deshalb werden wir diese Liste regelmäßig aktualisieren. Verwendete Informationskategorien: Die tatsächlich verwendeten Informationen sind von der jeweiligen rechtlichen Verpflichtung abhängig, können jedoch die folgenden Kategorien umfassen: Deine Konto-Informationen, Benutzerinhalte (sofern von einem Benutzer bereitgestellt), Konto-Zugriffsinformationen, Dein Netzwerk, Deine Community- und Gruppeninformationen, Informationen des Customer Supports und andere Mitteilungen, Nutzungsinformationen, Protokoll- und Problemlösungsinformationen, Geräte- und Verbindungsdaten, Allgemeine Standortinformationen, Meldungen von Benutzern, Benutzeroptionen, Cookies, Von anderen über dich bereitgestellte Informationen, Unternehmen auf WhatsApp, Dienste Dritter. Schutz deiner lebenswichtigen Interessen oder derjenigen einer anderen Person. Zum Schutz deiner lebenswichtigen Interessen oder derjenigen einer anderen Person. Wir wenden automatisierte Verarbeitungstechniken an und führen manuelle Prüfungen durch Menschen durch. Wir teilen Informationen mit Strafverfolgungsbehörden und anderen, wenn die lebenswichtigen Interessen einer Person geschützt werden müssen, etwa in einer Notsituation. Diese lebenswichtigen Interessen umfassen den Schutz des Lebens, der physischen oder psychischen Gesundheit, des Wohlbefindens oder der Integrität deiner Person oder eines anderen. Beim Schutz dieser lebenswichtigen Interessen sind wir bestrebt, schädliches Verhalten zu bekämpfen und Sicherheit und Integrität zu fördern. Beispielsweise untersuchen wir Meldungen von schädlichem Verhalten und ergreifen entsprechende Maßnahmen, etwa die Weitergabe von Informationen an die zuständigen Behörden, wenn das Risiko eines unmittelbar drohenden schädlichen Verhaltens wie eines Angriffs besteht oder wenn die Sicherheit einer Person gefährdet ist. Zudem vergleichen wir Profilbilder, Community- und Gruppenbilder und gemeldete Bilder mit einer Datenbank mit bekanntem Material über den sexuellen Missbrauch von Kindern in gehashter Form und verwenden eine Kombination aus automatisierten Verarbeitungstechniken und menschlichen Überprüfungen, um bisher nicht bekanntes Material über den sexuellen Missbrauch von Kindern in diesen Bildern zu erkennen. Wenn wir potenzielles Material über den sexuellen Missbrauch von Kindern entdecken, melden wir dieses an das National Center for Missing & Exploited Children (mehr dazu, wie wir Kinderausbeutung bekämpfen, erfährst du hier). Kategorien: Deine Konto-Informationen, Benutzerinhalte (sofern von einem Benutzer bereitgestellt), Dein Netzwerk, Deine Community- und Gruppeninformationen, Informationen des Customer Supports und andere Mitteilungen, Nutzungsinformationen, Protokoll- und Problemlösungsinformationen, Geräte- und Verbindungsdaten, Allgemeine Standortinformationen, Cookies, Benutzeroptionen, Von anderen über dich bereitgestellte Informationen, Meldungen von Benutzern, Unternehmen auf WhatsApp, Dienste Dritter. Berechtigte Interessen: Wir stützen uns auf unsere berechtigten Interessen bzw. die berechtigten Interessen eines Dritten, wie z. B. unsere Benutzer, sofern nicht deine Interessen oder Grundrechte und Grundfreiheiten überwiegen („berechtigten Interessen“): Warum und wie wir deine Informationen verarbeiten: Business Intelligence und Analytics: Wir zählen Benutzer und Ereignisse zwecks Reporting, um zu ermitteln, wie viele Benutzer WhatsApp hat (und ähnliche Metriken), damit wir diese Metriken an verbundene Unternehmen, Aufsichtsbehörden und die Öffentlichkeit weitergeben können. Dies umfasst Metriken wie die Anzahl der einzigartigen Benutzer von WhatsApp innerhalb der Meta-Unternehmen. Diese ermitteln wir, indem wir feststellen, welche unserer Benutzer keine anderen Meta-Apps verwenden. Wir validieren Metriken, um herauszufinden, wie und wie oft unsere Dienste genutzt werden und wie sie im Vergleich zur Nutzung in den Meta-Unternehmen abschneiden, um die Produktausrichtung und -entwicklung zu unterstützen und zu verbessern und die zukünftige Akzeptanz von Diensten oder Funktionen vorherzusagen. Berechtigtes Interesse: Es liegt in unserem Interesse, die Nutzung unserer Dienste zu messen und die Personen zu zählen, die mit den WhatsApp-Diensten interagieren, um die Produktausrichtung und -entwicklung zu unterstützen und zu verbessern und die Bereitstellung eines präzisen und zuverlässigen Reportings zu ermöglichen. Kategorien: Business Intelligence und Analytics: Deine Konto-Informationen, Deine

Community- und Gruppeninformationen, Informationen des Customer Supports und andere Mitteilungen, Nutzungsinformationen, Protokoll- und Problemlösungsinformationen, Geräte- und Verbindungsdaten, Allgemeine Standortinformationen, Benutzeroptionen. Wir speichern und teilen Informationen mit anderen, einschließlich Strafverfolgungsbehörden, und um auf rechtliche Anfragen zu reagieren. Dies umfasst die Reaktion auf rechtliche Anfragen, wo wir zwar nicht durch anwendbares Recht dazu gezwungen sind, aber in gutem Glauben der Ansicht sind, dass dies gemäß dem Recht des jeweiligen Staates erforderlich ist, oder das Teilen von Informationen mit Strafverfolgungsbehörden oder Branchenpartnern (z. B. mit anderen Online-Plattformen und Technologieunternehmen), um missbräuchliches oder rechtswidriges Verhalten zu bekämpfen. Beispielsweise speichern wir einen Schnappschuss von Benutzerinformationen, wenn dies von Strafverfolgungsbehörden gefordert wird und für die Zwecke einer Untersuchung notwendig ist. Wir können außerdem rechtswidrige oder gegen die Bestimmungen verstoßende Inhalte an Strafverfolgungs-, staatliche oder andere Behörden melden. Es liegt in unserem Interesse und in dem von WhatsApp-Benutzern, Betrug, unbefugte Nutzung von WhatsApp, Verstöße gegen unsere Bedingungen und Richtlinien und andere schädliche oder rechtswidrige Aktivitäten zu verhindern und zu verfolgen. Es liegt in unserem Interesse, uns selbst (insbesondere unsere Rechte, unsere Mitarbeiter, unser Eigentum oder unsere Produkte), unsere Benutzer oder andere Personen zu schützen, unter anderem im Rahmen von Untersuchungen oder behördlichen Anfragen, oder um Tod oder eine unmittelbar bevorstehende Körperverletzung abzuwenden. Die Öffentlichkeit sowie Branchenpartner (z. B. andere Online-Plattformen und Technologieunternehmen) haben ein berechtigtes Interesse daran, dass missbräuchliches oder rechtswidriges Verhalten untersucht und bekämpft wird. Die tatsächlich verwendeten Informationen sind von den tatsächlichen Umständen abhängig, können jedoch die folgenden Kategorien umfassen: Deine Konto-Informationen, Dein Netzwerk, Deine Community- und Gruppeninformationen, Informationen des Customer Supports und andere Mitteilungen, Protokoll- und Problemlösungsinformationen, Geräte- und Verbindungsdaten, Nutzungsinformationen, Allgemeine Standortinformationen, Meldungen von Benutzern. Wir speichern und teilen Informationen, wenn wir juristischen Rat suchen oder uns selbst im Kontext von Gerichtsverfahren oder anderen Streitigkeiten schützen müssen. Dies umfasst Angelegenheiten wie Verstöße gegen unsere Bedingungen und Richtlinien. Es liegt in unserem Interesse und in dem von WhatsApp-Benutzern, auf Beschwerden zu reagieren, Betrug, unbefugte Nutzung von WhatsApp, Verstöße gegen unsere Bedingungen und Richtlinien und andere schädliche oder rechtswidrige Aktivitäten zu verhindern und zu verfolgen. Es liegt in unserem Interesse, juristischen Rat zu suchen und uns selbst (insbesondere unsere Rechte, unsere Mitarbeiter, unser Eigentum oder unsere Produkte), unsere Benutzer oder andere Personen zu schützen, unter anderem im Rahmen von Untersuchungen oder behördlichen Anfragen sowie Gerichtsverfahren oder anderen Streitigkeiten. Die tatsächlich verwendeten Informationen sind von den tatsächlichen Umständen abhängig, können jedoch die folgenden Kategorien umfassen: Deine Konto-Informationen, Benutzerinhalte (sofern von einem Benutzer bereitgestellt), Dein Netzwerk, Deine Community- und Gruppeninformationen, Informationen des Customer Supports und andere Mitteilungen, Nutzungsinformationen, Protokoll- und Problemlösungsinformationen, Geräte- und Verbindungsdaten, Cookies, Benutzeroptionen, Von anderen über dich bereitgestellte Informationen, Meldungen von Benutzern, Unternehmen auf WhatsApp, Dienste Dritter. Zur Förderung von Sicherheit und Integrität außerhalb der Erfüllung unseres Vertrags mir dir tun wir Folgendes: Protokollieren von Meldungen von Benutzern und Mustern von Konto-Kompromittierungen, um die Techniken zu verstehen, die von den Übeltätern, welche die Dienste stören, genutzt werden. Analysieren der Geräte- und Verbindungsdaten von Benutzern, um Muster von verdächtigem Verhalten oder Verstöße gegen unsere Richtlinien und Bedingungen zu identifizieren und zu untersuchen. Zum Schutz der Sicherheit und Integrität unserer Dienste: Deine Konto-Informationen, Dein Netzwerk, Deine Community- und Gruppeninformationen, Nutzungsinformationen, Protokoll- und Problemlösungsinformationen, Geräte- und Verbindungsdaten, Meldungen von Benutzern. Zur Verbesserung des WhatsApp Customer Supports tun wir Folgendes: Nachverfolgen von Informationen über deine Interaktionen mit unserem Customer Support, um zu erfahren, ob Probleme zeitnah gelöst werden und die in unseren FAQ bereitgestellten Informationen hilfreich sind. Ausführen von Qualitätssicherungsprüfungen für die Interaktionen mit unseren Kunden. Anfordern und Prüfen von Informationen, die du in Umfragen zur Kundenzufriedenheit angibst. Protokollieren von Suchanfragen in unserem Hilfebereich, um einen Index häufiger Suchanfragen zu erstellen und die Inhalte unseres Hilfebereichs aktuell zu halten. Zur Verbesserung des WhatsApp Customer Supports: Deine Konto-Informationen, Informationen des Customer Supports und andere Mitteilungen, Nutzungsinformationen, Protokoll- und Problemlösungsinformationen, Geräte- und Verbindungsdaten, Allgemeine Standortinformationen, Cookies, Meldungen von Benutzern Du hast das Recht, dieser Verarbeitung zu widersprechen und ihre Einschränkung zu verlangen. Wenn du deine Rechte ausüben möchtest, lies bitte den Abschnitt So übst du deine Rechte aus dieser Datenschutzrichtlinie. Wir gestatten weiterhin keine Werbebanner von Dritten in unseren Diensten. Wir

haben keine Absicht sie einzuführen. Sollten wir es jedoch jemals beabsichtigen, werden wir diese Datenschutzrichtlinie aktualisieren. So übst du deine Rechte aus: Nach anwendbarem Datenschutzrecht hast du das Recht auf Auskunft, Berichtigung, Übertragbarkeit bzw. Löschung deiner Informationen sowie das Recht, bestimmte Verarbeitungen deiner Informationen einzuschränken bzw. ihnen zu widersprechen. Dies umfasst auch das Recht, unserer Verarbeitung deiner Informationen für Direktwerbung zu widersprechen und das Recht, unserer Verarbeitung deiner Informationen zu widersprechen, wenn wir unsere berechtigten Interessen bzw. die eines Dritten verfolgen. Wir werden verschiedene Faktoren berücksichtigen, wenn wir einen Widerspruch bewerten, unter anderem: deine vernünftigen Erwartungen, den Nutzen und die Risiken für dich, uns, andere Benutzer oder Dritte sowie sonstige verfügbare Mittel zur Erreichung desselben Zwecks, die möglicherweise weniger invasiv sind und keine unverhältnismäßigen Anstrengungen erfordern. Deinem Widerspruch wird stattgegeben, und wir werden die Verarbeitung deiner Informationen einstellen, es sei denn, die Verarbeitung basiert auf zwingenden berechtigten Gründen oder ist aus rechtlichen Gründen erforderlich. Hier kannst du unserer Verarbeitung deiner Informationen widersprechen und mehr über deine Optionen zur Einschränkung unserer Möglichkeiten zur Verwendung deiner Informationen erfahren. Wenn wir deine Informationen für Direktwerbung verwenden, kannst du jederzeit widersprechen und künftige Marketingmitteilungen abbestellen, indem du den in solchen Mitteilungen enthaltenen Link zum Abbestellen oder unsere In-App-Funktion „Blockieren“ nutzt. Du kannst auf deine Informationen zugreifen bzw. sie übertragen, indem du unsere In-App-Funktion „Konto-Info anfordern“ (verfügbar unter Einstellungen > Konto) nutzt. Wie im Abschnitt Aufbewahrung deiner Informationen beschrieben, kannst du direkt in der App auf Funktionen zugreifen, um deine Informationen zu berichtigen, zu aktualisieren und zu löschen. Wenn wir von dir bereitgestellte Informationen auf Grundlage deiner Einwilligung verarbeiten, hast du das Recht, diese Einwilligung jederzeit zu widerrufen; dies berührt dann allerdings nicht die Rechtmäßigkeit der auf Grundlage der Einwilligung erfolgten Verarbeitung vor ihrem Widerruf. Wenn du deine Einwilligung widerrufen möchtest, öffne die Einstellungen deines Geräts oder deine In-App-Einstellungen. Du hast das Recht, eine Beschwerde gemäß der DSGVO bei der für WhatsApp zuständigen federführenden Aufsichtsbehörde, der irischen Datenschutzkommission (Irish Data Protection Commission) oder bei einer anderen zuständigen Datenschutz-Aufsichtsbehörde einzureichen. Aufbewahrung deiner Informationen: Wir bewahren Informationen so lange wie für die in dieser Datenschutzrichtlinie dargelegten Zwecke erforderlich auf, insbesondere zur Bereitstellung unserer Dienste oder zu anderen rechtmäßigen Zwecken, etwa zur Erfüllung rechtlicher Verpflichtungen, zur Durchsetzung unserer Bedingungen und zur Vermeidung von Verstößen gegen diese sowie zur Bekämpfung von Spam und zum Schutz oder zur Verteidigung unserer Rechte, unseres Eigentums und unserer Benutzer. Die Dauer der Aufbewahrung wird von Fall zu Fall bestimmt und hängt von den folgenden Faktoren ab: Der Art der Informationen und dem Grund ihrer Erfassung und Verarbeitung. Die Dauer der Aufbewahrung deiner Informationen wird in der Regel dadurch bestimmt, wie lange wir diese Informationen benötigen, um dir unsere Dienste, einschließlich jeglicher von dir verwendeter optionaler Funktionen, und Customer Support bereitzustellen. Beispiel: Wie oben beschrieben benötigen wir bestimmte deiner Konto-Informationen, um unsere Dienste bereitstellen zu können. Diese müssen wir zur Aufrechterhaltung deines Kontos aufbewahren, solange dein Konto besteht. Wir speichern deine Benutzeroptionen, solange dein Konto besteht. Wir bewahren Authentifizierungsinformationen auf, solange dein Konto besteht. Andere Informationen müssen wir nur so lange aufbewahren wie erforderlich, um dir optionale Funktionen bereitzustellen, etwa dein Netzwerk, solange du den Kontakt-Upload verwendest. Wir bewahren Informationen, die mithilfe von Cookies erfasst wurden, 90 Tage lang auf. Wir bewahren Kommunikation mit dem Customer Support im Allgemeinen 30 Tage lang auf, nachdem sie bearbeitet wurde, oder 90 Tage lang, nachdem wir sie erhalten haben, je nachdem, welcher Zeitpunkt früher eintritt. Wir bewahren Meldungen von Benutzern im Allgemeinen 90 Tage lang auf. In bestimmten Fällen müssen wir deine Informationen aus rechtlichen Gründen länger aufbewahren, wie im Abschnitt „Rechtliche Gründe“ unten beschrieben. Rechtliche Gründe. In bestimmten Fällen bewahren wir deine Informationen auch aus rechtlichen Gründen auf, selbst nachdem dein Konto gelöscht wurde. Wir bewahren deine Informationen auf: Um auf eine rechtliche Anfrage zu reagieren oder geltendes Recht zu beachten, wenn wir rechtlich dazu verpflichtet sind, Informationen zu speichern. Wenn wir beispielsweise eine rechtsgültige Anfrage im Zusammenhang mit deinem Konto erhalten, etwa einen Beweissicherungsbeschluss oder einen Durchsuchungsbefehl, bewahren wir deine Informationen auf, nachdem du dein Konto gelöscht hast. Um Anfragen und Beschwerden zu bearbeiten und beizulegen. Beispielsweise bewahren wir Korrespondenz im Zusammenhang mit Anfragen betroffener Personen gemäß der DSGVO ein Jahr lang auf, falls die entsprechenden Anfragen nicht abschließend bearbeitet werden können und diese Korrespondenz erforderlich ist, um daraus resultierende Beschwerden zu bearbeiten. In solchen Fällen wird die Korrespondenz aufbewahrt, während die entsprechenden Beschwerden beigelegt werden. Für Rechtsstreitigkeiten oder aufsichtsrechtliche

Angelegenheiten. Beispielsweise bewahren wir deine Informationen auf, wenn dies im Zusammenhang mit einem rechtlichen Anspruch oder einer Beschwerde vernünftigerweise erforderlich ist, etwa wenn wir Gegenstand einer behördlichen Untersuchung werden oder uns in Gerichtsverfahren wegen eines Anspruchs im Zusammenhang mit deinen Informationen verteidigen müssen oder einer Aufsichtsbehörde im Hinblick auf eine Beschwerde antworten müssen, die von einer anderen Person vorgenommen wurde. Fragen im Zusammenhang mit der Sicherheit und Integrität unserer Dienste und zum Schutz von Rechten, Eigentum und Benutzern. Zum Beispiel speichern wir Informationen, die für die Untersuchung des Missbrauchs unserer Dienste, wie Spam und andere schlechte Erfahrungen, erforderlich sind. Wenn wir ein Konto deaktivieren, weil es gegen unsere Bedingungen verstößt, bewahren wir die Informationen über diesen Benutzer aus Gründen der Sicherheit und Integrität auf. Die tatsächlich von uns aufbewahrten Informationen und die Dauer ihrer Aufbewahrung hängen von der Art des entsprechenden Grundes ab. Betriebliche Erfordernisse für die Aufbewahrung. Wir müssen Informationen in bestimmten Fällen aus betrieblichen Gründen aufbewahren. Kann eine Nachricht beispielsweise nicht sofort zugestellt werden, speichern wir sie bis zu 30 Tage in verschlüsselter Form auf unseren Servern und versuchen in dieser Zeit, sie zuzustellen. Zudem speichern wir Informationen bei Bedarf zur Problemlösung und zum Debugging von Problemen mit den Diensten. Wir bewahren die zu diesem Zweck gespeicherten Informationen bis zu 90 Tage lang auf, sofern keine längere Speicherung zur Untersuchung und Lösung eines spezifischen Problems oder aus rechtlichen Gründen erforderlich ist. Nachrichten. Wir bewahren Informationen, die wir verarbeiten, um deine Nachrichten oder Anrufe zu übermitteln (dies umfasst Informationen wie deine Telefonnummer, Datum und Uhrzeit eines Anrufs oder einer Nachricht oder die Dauer deiner Anrufe), entsprechend den spezifischen Regeln und Anforderungen unter der EU-Richtlinie 2002/58/EG auf, sofern anwendbar, und zwar so lange wie notwendig, um die Kommunikation zu übermitteln, unsere Dienste zu betreiben, die Sicherheit unserer Dienste sicherzustellen oder rechtliche Verpflichtungen gemäß anwendbarem Recht zu erfüllen. Wenn wir die Informationen nicht mehr zu einem dieser Zwecke benötigen, löschen oder anonymisieren wir sie. Löschen deiner Informationen: Was passiert mit deinen Informationen, wenn dein Konto gelöscht wird? Wenn du dein WhatsApp-Konto löschst oder wenn es aufgrund von Inaktivität gelöscht wird (Informationen zu inaktiven Konten findest du unter Über die Löschung inaktiver Konten), löschen wir die Informationen, die wir über dich haben, abgesehen von den unten aufgeführten Informationen, die wir unter bestimmten Umständen aufbewahren. Gelöschte Informationen. Deine Konto-Informationen und nicht an dich zugestellte Nachrichten werden von unseren Servern gelöscht. Du wirst aus allen WhatsApp-Communitys und -Gruppen entfernt. Bitte beachte, dass es aus technischen Gründen ab dem Start des Löschmodens bis zu 90 Tage dauern kann, bis deine WhatsApp-Informationen gelöscht oder anonymisiert sind. Auch nach den 90 Tagen verbleiben möglicherweise Kopien deiner Informationen für eine begrenzte Zeit im Backup-Speicher, den wir im Notfall, nach einem Softwarefehler oder einem anderen Datenverlust zur Wiederherstellung verwenden. Informationen, die wir nach der Löschung deines Kontos aufbewahren. Wenn wir einen Sicherheitsvorfall analysieren oder untersuchen, müssen wir zur Aufrechterhaltung der Sicherheit unserer Dienste Protokoll- und Problemlösungsinformationen im Zusammenhang mit dem geprüften Vorfall über den normalen 90-Tage-Zeitraum hinaus aufbewahren. Kopien bestimmter Protokoll Datensätze verbleiben in unserer Datenbank, werden jedoch von persönlichen Kennungen getrennt und verwendet, um beispielsweise die Performance, Zuverlässigkeit und Effizienz zu messen sowie unsere Dienste zu betreiben und zu verbessern. Dein Konto war ursprünglich durch zufällig generierte Kennungen mit diesen Datensätzen verknüpft. Um diese Informationen zu trennen, wenn dein Konto gelöscht wird, löschen wir die Verknüpfung zwischen dieser Kennung und deinem Konto im Rahmen der Konto-Löschung. Kopien deiner Informationen können auch aus rechtlichen Gründen unter den beschriebenen Umständen nach der Löschung deines Kontos aufbewahrt werden. Die möglicherweise aufbewahrten Informationen sowie deren Aufbewahrungszeit sind von den spezifischen rechtlichen Gründen abhängig, aus denen wir sie aufbewahren müssen. Weitere Informationen dazu, wie lange wir Informationen speichern, findest du unter Aufbewahrung deiner Informationen. Verwaltung deiner Informationen: Wenn du deine Informationen verwalten, ändern, einschränken oder löschen möchtest, kannst du dies über die folgenden Funktionen tun: Einstellungen. Du kannst deine Einstellungen ändern, um bestimmte Informationen zu verwalten, die für andere Benutzer verfügbar sind. Du kannst deine Kontakte, Gruppen und Broadcast-Listen verwalten oder unsere „Blockieren“-Funktion nutzen, um zu verwalten, mit wem du auf unseren Diensten kommunizieren möchtest. Ändern deiner Mobiltelefonnummer, deines Profilnamens und Profilbildes und deiner Info. Wenn du deine Mobiltelefonnummer ändern möchtest, musst du sie über unsere In-App-Funktion „Nummer ändern“ aktualisieren; anschließend musst du dein Konto auf deine neue Mobiltelefonnummer übertragen. Du kannst auch jederzeit deinen Profilnamen, dein Profilbild und deine Info ändern. Löschen deines WhatsApp-Kontos. Du kannst dein WhatsApp-Konto jederzeit über unsere In-App-Funktion „Mein Konto löschen“ in deinen In-App-Einstellungen löschen. Sobald du den Löschmodens deines Kontos einleitest, kann dieses Konto nicht

mehr genutzt werden (d. h., du kannst dich dann nicht mehr anmelden oder erneut registrieren oder auf Inhalte, darunter den Nachrichtenverlauf, zugreifen, da diese gelöscht werden). Im Abschnitt Löschen deiner Informationen findest du weitere Informationen darüber, was mit deinen Informationen geschieht, wenn du dein Konto löschst. Beachte, dass die Informationen, die wir erheben, noch länger auf unseren Servern gespeichert werden, wenn du lediglich WhatsApp von deinem Gerät löschst, ohne die In-App-Funktion „Mein Konto löschen“ zu nutzen. WhatsApp-Konten werden in der Regel nach einer Inaktivität von 120 Tagen gelöscht. Benutzer werden vorher nicht gewarnt. Weitere Informationen findest du im Artikel Über die Löschung inaktiver Konten in unserem Hilfebereich. Bitte bedenke auch, dass das Löschen deines Kontos nicht diejenigen deiner Informationen beeinflusst, die mit den von dir erstellten Communitys oder Gruppen zusammenhängen (etwa Community- oder Gruppennamen) oder die andere Benutzer in Bezug auf dich haben, wie beispielsweise ihre Kopien der Nachrichten, die du ihnen gesendet hast. Zusammenarbeit mit Behörden, Beratern und Branchenpartnern: Wir rufen deine im Abschnitt Informationen, die wir erheben beschriebenen Informationen auf und teilen sie, unter anderem mit Aufsichtsbehörden, Strafverfolgungsbehörden, anderen staatlichen Behörden, Branchenpartnern (z. B. andere Online-Plattformen und Technologieunternehmen), unseren Beratern (z. B. externe Anwälte, die für uns tätig sind) und anderen entsprechend dem Abschnitt Wie und warum wir deine Informationen verarbeiten; unsere Rechtsgrundlagen für die Verarbeitung, wenn wir in gutem Glauben der Ansicht sind, dass dies zu folgenden Zwecken notwendig ist: Reaktion gemäß anwendbaren Gesetzen oder Vorschriften, gerichtlichen Anordnungen, rechtlichen Verfahren oder Behördenanfragen. Beispielsweise die Weitergabe an Aufsichtsbehörden, Strafverfolgungsbehörden oder andere staatliche Behörden als Reaktion auf rechtliche Anfragen oder die Weitergabe an Parteien in einem Zivilprozess gemäß gerichtlichen Anordnungen; Erkennung, Untersuchung, Verhinderung oder Verfolgung bzw. Behebung von Betrug oder anderen unrechtmäßigen Aktivitäten oder Sicherheits- und technischen Problemen. Beispielsweise rufen wir Informationen auf und teilen sie mit Strafverfolgungsbehörden, anderen staatlichen Behörden oder Branchenpartnern (z. B. andere Online-Plattformen und Technologieunternehmen), um Übeltäter zu ermitteln, die unsere Dienste zu unrechtmäßigen Zwecken nutzen, und um dem vorzubeugen; oder Schutz der Rechte, des Eigentums und der Sicherheit von unseren Benutzern, WhatsApp, den Meta-Unternehmen oder anderen, unter anderem um Tod oder eine drohende Körperverletzung abzuwenden. Beispielsweise die Weitergabe an Strafverfolgungsbehörden in Notfallsituationen, in denen das Leben einer Person bedroht ist. Weitere Informationen dazu, wie wir deine Informationen zu diesen Zwecken aufbewahren, findest du im Abschnitt Aufbewahrung deiner Informationen. Unsere Verarbeitung hängt von den jeweiligen Umständen ab. Weitere Informationen zu den verschiedenen Kategorien der betroffenen Informationen und zu den Rechtsgrundlagen, auf die wir uns stützen, findest du im Abschnitt Wie und warum wir deine Informationen verarbeiten; unsere Rechtsgrundlagen für die Verarbeitung unter den Überschriften „Verarbeitung erforderlich zur Erfüllung unseres Vertrags mit dir“, „Erfüllung einer rechtlichen Verpflichtung“, „Schutz deiner lebenswichtigen Interessen oder derjenigen einer anderen Person“ und „Berechtigte Interessen“. Übermittlung von Informationen in Länder außerhalb des EWR im Rahmen unserer globalen Aktivitäten. Warum werden Informationen in Länder außerhalb des Europäischen Wirtschaftsraums übermittelt, und in welche Länder werden sie übermittelt? WhatsApp teilt die im Abschnitt Informationen, die wir erheben, dieser Datenschutzrichtlinie beschriebenen Informationen weltweit, sowohl intern mit den Meta-Unternehmen als auch extern mit Dritten entsprechend dieser Datenschutzrichtlinie und unseren Bedingungen. Dies umfasst Orte, an denen sich die Rechenzentren befinden, mit denen wir arbeiten, und an denen unsere anderen internen Meta-Unternehmen und externen Drittdienstleister ansässig sind (dies umfasst die Vereinigten Staaten). Diese Übermittlungen sind erforderlich und unerlässlich, um die in unseren Bedingungen dargelegten Dienste bereitzustellen und um unsere Dienste global zu betreiben und bereitzustellen, damit du auf der ganzen Welt auf WhatsApp mit Benutzern und Unternehmen kommunizieren kannst. Wie schützen wir deine Informationen? Wenn Informationen, die von WhatsApp kontrolliert werden, in die Vereinigten Staaten oder andere Drittländer außerhalb des Europäischen Wirtschaftsraums übertragen oder übermittelt bzw. dort gespeichert und verarbeitet werden, nutzen wir die folgenden Übertragungsmechanismen: Angemessenheitsbeschlüsse: Wir stützen uns auf Beschlüsse der Europäischen Kommission, in denen anerkannt wird, dass bestimmte Länder und Territorien außerhalb des Europäischen Wirtschaftsraums einen angemessenen Schutz personenbezogener Informationen sicherstellen. Diese Beschlüsse werden als „Angemessenheitsbeschlüsse“ bezeichnet. Wir übertragen deine Konto-Informationen, Geräte- und Verbindungsdaten, Nutzungsinformationen und Benutzeroptionen (siehe Informationen, die wir erheben) auf Grundlage des Angemessenheitsbeschlusses der Europäischen Kommission für Israel aus dem Europäischen Wirtschaftsraum nach Israel. Standardvertragsklauseln: Wir verwenden von der Europäischen Kommission genehmigte Standardvertragsklauseln (und gegebenenfalls die Standardvertragsklauseln für das Vereinigte Königreich) für Übertragungen in die Vereinigten Staaten,

in das Vereinigte Königreich und nach Singapur. Beispielsweise nutzt WhatsApp die globale Infrastruktur und die Rechenzentren von Meta, die sich auf der ganzen Welt, einschließlich in den Vereinigten Staaten, befinden, um die im Abschnitt Informationen, die wir erheben dieser Datenschutzrichtlinie beschriebenen Informationen zu speichern. Um eine Kopie der Standardvertragsklauseln zu erhalten, lies bitte den Artikel „Standardvertragsklauseln“ in unserem Hilfebereich. Während Übermittlungen in Länder, für die es keinen Angemessenheitsbeschluss gibt, in der Regel auf der Grundlage der Standardvertragsklauseln erfolgen, können Übermittlungen unter bestimmten Umständen auch auf der Grundlage von Ausnahmen stattfinden, die im Rahmen des Datenschutzrechts vorgesehen sind. Beispielsweise die Weitergabe an Strafverfolgungsbehörden in Notfallsituationen, in denen das Leben einer Person bedroht ist. Wenn du irgendwelche Fragen zu den Standardvertragsklauseln hast, kannst du uns kontaktieren. Aktualisierungen unserer Datenschutzrichtlinie: Wir können unsere Datenschutzrichtlinie ändern oder aktualisieren. Wir werden dich ggf. von Änderungen an dieser Datenschutzrichtlinie in Kenntnis setzen und das Datum „Letzte Änderung“ oben in dieser Datenschutzrichtlinie aktualisieren. Bitte lies dir unsere Datenschutzrichtlinie von Zeit zu Zeit erneut durch. Kontaktaufnahme mit uns: Der Datenschutzbeauftragte für WhatsApp kann hier kontaktiert werden. Solltest du Fragen zu unserer Datenschutzrichtlinie haben, kontaktiere uns bitte oder schreibe uns unter: WhatsApp Ireland Limited, Attn: Privacy Policy, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland

LinkedIn Datenschutzerklärung

Der Schutz Ihrer Daten ist uns wichtig. LinkedIn hat es sich zur Aufgabe gemacht, Fach- und Führungskräfte weltweit miteinander zu vernetzen, um ihnen zu noch mehr Produktivität und Erfolg zu verhelfen. In diesem Rahmen verpflichten wir uns, transparent zu machen, welche Daten wir über Sie sammeln, wie sie verwendet und mit wem sie geteilt werden. Wenn Sie unsere Dienste nutzen, erfolgt dies auf Grundlage unserer Datenschutzrichtlinie (siehe nachfolgende Beschreibung). Wir geben unseren Nutzerinnen und Nutzern die Möglichkeit, Einstellungen bezüglich der Daten vorzunehmen, die wir wie in dieser Datenschutzrichtlinie, der Cookie-Richtlinie, den Einstellungen und dem Hilfebereich beschrieben erfassen, nutzen und teilen. Zentrale Begriffe: Inhalt: Von uns erfasste Informationen, Verwendung Ihrer Daten, Teilen Ihrer Daten, Ihre Optionen und Pflichten Weitere wichtige Informationen. Vorwort: LinkedIn ist ein soziales Netzwerk und eine Online-Plattform für Fach- und Führungskräfte. Menschen nutzen unsere Dienste, um Geschäftschancen und Informationen zu finden, um selbst gefunden zu werden und um sich mit anderen Personen zu vernetzen. Unsere Datenschutzrichtlinie gilt für alle Mitglieder oder Besucher unserer Dienste. Bei uns registrierte Nutzerinnen und Nutzer („Mitglieder“) teilen ihre berufliche Identität, interagieren mit ihrem Netzwerk, tauschen Wissen und berufliche Einblicke aus, veröffentlichen und lesen relevante Inhalte, entwickeln und erweitern Kompetenzen und finden Geschäfts- und Karrierechancen. Die Inhalte und Daten einiger unserer Dienste sind für Nichtmitglieder („Besucher“) einsehbar. Mit dem Begriff „designierte Länder“ sind die Länder der Europäischen Union (EU) und des Europäischen Wirtschaftsraumes (EWR) sowie die Schweiz gemeint. Dienste: Diese Datenschutzrichtlinie, einschließlich unserer Cookie-Richtlinie, bezieht sich auf Ihre Nutzung unserer Dienste. Diese Datenschutzrichtlinie gilt für LinkedIn.com, Apps mit dem Markenzeichen von LinkedIn, LinkedIn Learning sowie andere mit LinkedIn verbundene Websites, Apps, Informationen und Dienste („Dienste“), einschließlich Offsite-Dienste wie unsere Anzeigendienste sowie die Plug-ins „Mit LinkedIn bewerben“ und „Auf LinkedIn teilen“, aber unter Ausschluss von Diensten, bei denen angegeben wird, dass für sie eine andere Datenschutzrichtlinie gilt. Personen mit Wohnsitz in Kalifornien finden zusätzliche Offenlegungen, die nach kalifornischem Recht erforderlich sind, in unserem Dokument mit Informationen zum Datenschutz in Kalifornien (California Privacy Disclosure). Datenverantwortliche und Vertragspartner: Wenn Sie sich in den „designierten Ländern“ befinden, wird LinkedIn Ireland Unlimited Company („LinkedIn Ireland“) zum Verantwortlichen für Ihre personenbezogenen Daten, die unseren Diensten bereitgestellt, für oder durch diese erfasst oder im Zusammenhang mit ihnen verarbeitet werden. Wenn Sie sich außerhalb der „designierten Länder“ befinden, ist LinkedIn Corporation der Verantwortliche für Ihre personenbezogenen Daten, die unseren Diensten bereitgestellt, für oder durch diese erfasst oder im Zusammenhang mit ihnen verarbeitet werden. Als Besucher oder Mitglied unserer Dienste unterliegt die Erfassung, Nutzung und Weitergabe Ihrer personenbezogenen Daten dieser Datenschutzrichtlinie sowie anderen in dieser Datenschutzrichtlinie genannten Dokumenten und deren Aktualisierungen. Ändern: Änderungen an dieser Datenschutzrichtlinie gelten für Ihre Nutzung unserer Dienste ab dem „Datum des Inkrafttretens“. LinkedIn („wir“ oder „uns“) steht es frei, an dieser Datenschutzrichtlinie Änderungen vorzunehmen. Sollten wir wesentliche Änderungen vornehmen, benachrichtigen wir Sie über unsere Dienste oder auf andere Art und Weise, damit Sie Gelegenheit haben, die Änderungen zu überprüfen, bevor sie in Kraft treten. Wenn Sie mit irgendwelchen Änderungen nicht einverstanden sind, können Sie Ihr Konto schließen. Sie erkennen an, dass durch Ihre weitere Nutzung unserer Dienste nach Veröffentlichung der Änderungen an unserer Datenschutzrichtlinie oder der Benachrichtigung über diese Änderungen die Erfassung, Nutzung und Weitergabe Ihrer personenbezogenen Daten der aktualisierten Datenschutzrichtlinie ab dem Datum ihres Inkrafttretens unterliegt. Von uns erfasste Informationen: Von Ihnen bereitgestellte Informationen: Sie stellen Daten bereit, um ein Konto bei uns zu erstellen. Registrierung: Zur Erstellung eines Kontos müssen Sie Daten bereitstellen, einschließlich Ihres Namens, Ihrer E-Mail-Adresse und/oder Ihrer Handynummer und eines Passworts. Wenn Sie sich für einen Premium-Dienst registrieren, müssen Sie Zahlungs- und Rechnungsinformationen (z. B. Kreditkartendaten) angeben. Sie erstellen Ihr Profil auf LinkedIn (mit einem vollständigen Profil nutzen Sie unsere Dienste optimal). Profil: Welche Informationen Sie in Ihrem Profil veröffentlichen, beispielsweise Ausbildung, Berufserfahrung, Kenntnisse, Foto, Standort oder Region und Kenntnisbestätigungen, bleibt Ihnen überlassen. Mitglieder können auf Wunsch auch ein separates ProFinder-Profil erstellen. Sie sind nicht verpflichtet, auf Ihrem Profil zusätzliche Informationen anzugeben. Solche Profilinformationen tragen jedoch dazu bei, dass Sie unsere Dienste besser nutzen können, z. B. weil Sie dadurch für Recruiter und Geschäftschancen besser auffindbar werden. Es bleibt Ihnen überlassen, ob Sie vertrauliche Informationen auf Ihrem Profil veröffentlichen oder nicht und ob Sie diese Informationen öffentlich zugänglich machen. Bitte fügen Sie keine personenbezogenen Daten zu Ihrem Profil hinzu, von denen Sie nicht möchten, dass sie öffentlich verfügbar sind, und posten Sie solche Daten nicht. Indem Sie beispielsweise Ihr Adressbuch oder Ihren Kalender synchronisieren, stellen Sie weitere Daten zur Verfügung. Veröffentlichen und

Hochladen: Wir erfassen Ihre personenbezogene Daten, wenn Sie diese auf unseren Diensten bereitstellen, posten oder hochladen, z. B. wenn Sie auf unseren Diensten ein Formular ausfüllen (beispielsweise unter Angabe demografischer Daten oder eines Gehalts), eine Umfrage ausfüllen, einen Lebenslauf einreichen oder eine Bewerbung ausfüllen. Wenn Sie Ihr Adressbuch importieren, erhalten wir Ihre Kontakte (einschließlich von Kontaktinformationen, die Ihre Dienstleister oder Ihre App automatisch zu Ihrem Adressbuch hinzugefügt haben, als Sie Adressen oder Nummern kontaktierten, die nicht bereits auf Ihrer Liste waren). Wenn Sie Ihre Kontakte oder Kalender mit unseren Diensten synchronisieren, erfassen wir die Daten Ihres Adressbuchs und Terminkalenders, damit wir Ihnen und anderen zur Erweiterung Ihres Netzwerks Kontakte vorschlagen und Informationen über Ereignisse bereitstellen können, z. B. Zeiten, Orte, Teilnehmer und Kontakte. Sie sind nicht verpflichtet, personenbezogene Daten zu posten oder hochzuladen, jedoch ist Ihre Fähigkeit, Ihr Netzwerk zu erweitern und mit Ihrem Netzwerk über unsere Dienste in Kontakt zu treten, in diesem Fall beschränkt. Informationen von Anderen: Andere Mitglieder können Sie in Beiträgen erwähnen oder über Sie schreiben. Inhalte und News: Sie und andere können Inhalte mit Informationen über Sie (im Rahmen von Artikeln, Beiträgen, Kommentaren, Videos) auf unseren Diensten veröffentlichen. Wir erfassen möglicherweise auch öffentlich verfügbare Informationen zu Ihrer Person, zum Beispiel berufsbezogene News und Erfolge, und stellen diese im Rahmen unserer Dienste bereit, einschließlich in an andere Personen gesendete Mitteilungen über Erwähnungen in den News, in Übereinstimmung mit Ihren Einstellungen. Andere Mitglieder synchronisieren möglicherweise ihre Kontakte oder Kalender mit unseren Diensten. Kontakt- und Kalenderdaten: Wir erhalten personenbezogene Daten (einschließlich Kontaktdaten) von Ihnen, wenn andere ihre Kontakt- oder Kalenderdaten mit unseren Diensten synchronisieren, ihre Kontakte Mitgliederprofilen zuordnen, Visitenkarten scannen und hochladen oder über unsere Dienste Nachrichten verschicken (einschließlich Einladungen oder Kontaktanfragen). Wenn Sie oder andere der Synchronisation von E-Mail-Konten mit unseren Diensten zustimmen, erfassen wir außerdem Informationen aus den „Kopfzeilen“ der E-Mails, die wir mit Mitgliederprofilen assoziieren können. Kunden und Partnerunternehmen stellen uns möglicherweise Daten bereit. Partner: Wir erhalten Ihre personenbezogenen Daten (z. B. Ihre Jobbezeichnung und Ihre berufliche E-Mail-Adresse), wenn Sie die Dienste unserer Kunden und Partner in Anspruch nehmen, wie Arbeitgeber, potenzielle Arbeitgeber und Bewerbermanagementsysteme, die uns Bewerbungsdaten bereitstellen. Verbundene Unternehmen und andere Dienste: Wir erhalten Daten zu Ihrer Person, wenn Sie andere Dienste in Anspruch nehmen, die wir oder mit uns verbundene Unternehmen, einschließlich Microsoft, bereitgestellt werden. Sie können sich beispielsweise dafür entscheiden, Informationen über Ihre Kontakte in Microsoft Apps und Diensten wie Outlook an uns zu senden, um die professionellen Netzwerkaktivitäten auf unseren Diensten zu verbessern. Nutzung der Dienste: Wir protokollieren Ihre Besuche und Nutzung unserer Dienste, einschließlich mobiler Apps. Wir protokollieren Nutzungsdaten, wenn Sie unsere Dienste einschließlich unserer Websites, App- und Plattformtechnologie besuchen oder anderweitig nutzen, wenn Sie beispielsweise Inhalte (wie Lernvideos) oder Anzeigen betrachten oder anklicken (innerhalb oder außerhalb unserer Websites und Apps), eine Suche ausführen, eine unserer Apps für Mobilgeräte installieren oder aktualisieren, Artikel teilen oder sich um eine Stelle bewerben. Wir verwenden Anmeldedaten, Cookies, Geräteinformationen und IP-Adressen, um Sie zu identifizieren und Ihre Nutzung zu protokollieren. Cookies und ähnliche Technologien: Wir erfassen Daten über Cookies und ähnliche Technologien. Wie in unserer Cookie-Richtlinie näher dargelegt, nutzen wir Cookies und ähnliche Technologien (z. B. Pixel und Anzeigen-Tags), um Daten zu sammeln (z. B. Geräte-IDs), um Sie und Ihr Gerät oder Ihre Geräte innerhalb und außerhalb von und übergreifend über verschiedene(n) Dienste(n) und Geräte(n) zu erkennen. Wir erlauben es auch bestimmten Dritten, in Übereinstimmung mit unserer Cookie-Richtlinie Cookies zu verwenden. Befinden Sie sich außerhalb der designierten Länder, erfassen wir auch Informationen zu Ihrem Gerät (oder verlassen uns auf andere, die diese erfassen), wenn Sie unsere Dienste nicht genutzt haben (z. B. Anzeigen-ID, IP-Adresse, Betriebssystem und Browserdaten), damit wir unseren Mitgliedern relevante Anzeigen zur Verfügung stellen und deren Wirksamkeit besser verstehen können. Mehr dazu. Sie können unsere Nutzung von Cookies und ähnlichen Technologien, die Ihr Verhalten auf anderen Websites für Zielgruppenwerbung und andere Werbezwecke verfolgen, ablehnen. Besucher finden diese Steuerelemente hier. Ihr Gerät und Standort: Wir erhalten Daten über Cookies und ähnliche Technologien. Wenn Sie unsere Dienste (einschließlich einiger Plug-ins und unserer Cookies oder ähnlicher Technologien auf den Websites Dritter) besuchen oder verlassen, erhalten wir sowohl die URL der Website, von der Sie kommen, als auch der Website, zu der Sie als Nächstes navigieren, sowie die Uhrzeit Ihres Besuchs. Wir erhalten auch Informationen über Ihr Netzwerk und Ihr Gerät (z. B. Ihre IP-Adresse, Ihren Proxy-Server, Ihr Betriebssystem, Ihren Webbrowser und Ihre Add-ons, Ihre Geräteerkennung und -funktionen, Ihre Cookie-IDs und/oder Ihren Internetanbieter bzw. Ihren Mobilfunkbetreiber). Greifen Sie auf unsere Dienste von einem Mobilgerät zu, sendet uns dieses Gerät auf Grundlage Ihrer Telefoneinstellungen

Daten über Ihren Standort. Wir fragen Sie nach Ihrer Zustimmung, bevor wir GPS oder andere Tools verwenden, um Ihren genauen Standort zu ermitteln. Nachrichten: Wir werden informiert, wenn Sie über unsere Dienste kommunizieren. Wir erfassen Informationen über Sie, wenn Sie in Verbindung mit unseren Diensten Nachrichten senden, erhalten oder mit Nachrichten interagieren. Erhalten Sie beispielsweise eine Kontaktanfrage auf LinkedIn, verfolgen wir, ob Sie darauf reagiert haben und senden Ihnen Erinnerungen. Mithilfe automatischer Scan-Technologie für Nachrichten unterstützen und schützen wir unsere Website. Beispielsweise setzen wir diese Technologie ein, um Ihnen mögliche Antworten auf Nachrichten vorzuschlagen und um Inhalte zu verwalten oder Inhalte auf unseren Diensten zu blockieren, die gegen unsere Nutzervereinbarung oder die Community-Richtlinien verstoßen. Vom Arbeitsplatz oder von der Ausbildungsstätte bereitgestellte Informationen: Wenn Ihre Organisation (z. B. Ihr Arbeitgeber oder Ihre Hoch- oder Berufsschule) für Sie einen Premium-Dienst kauft, übermittelt sie uns Daten zu Ihrer Person. Wenn andere, wie Ihr Arbeitgeber oder Ihre Ausbildungsstätte, unsere Dienste für Ihre Verwendung kaufen, übermitteln sie uns personenbezogene Daten über Sie und die Berechtigung zur Nutzung der Dienste durch ihre Angestellten, Studierenden oder Absolventen. Wir erhalten beispielsweise Kontaktdaten für die Admins von „Unternehmensseiten“ und wenn Personen die Berechtigung erhalten, unsere Premium-Dienste zu nutzen, wie z. B. unsere Recruiting-, Vertriebs- oder Lernprodukte. Websites und Dienste Dritter: Wir erhalten Daten, wenn Sie Websites besuchen, die unsere Anzeigen, Cookies oder einige unserer Plug-ins enthalten oder wenn Sie sich mit Ihrem LinkedIn Konto bei den Diensten Dritter einloggen. Wir erhalten Informationen über Ihre Besuche bei und Interaktionen mit von Dritten bereitgestellten Diensten, wenn Sie sich über LinkedIn einloggen oder die Dienste Dritter besuchen, die einige unserer Plug-ins (wie beispielsweise „Mit LinkedIn bewerben“) oder unsere Anzeigen, Cookies oder ähnliche Technologien enthalten. Sonstiges: Wir optimieren unsere Dienste, d. h. wir erhalten neue Daten und schaffen neue Wege zur Nutzung von Daten. Unsere Dienste sind dynamisch und wir führen oft neue Funktionen ein. Daher kann es vorkommen, dass neue Informationen erfasst werden müssen. Wenn wir andere wesentliche personenbezogene Daten erfassen oder wesentliche Änderungen daran vornehmen, wie wir Ihre Daten erfassen, verwenden oder teilen, benachrichtigen wir Sie und ändern unter Umständen auch diese Datenschutzrichtlinie. Zentrale Begriffe: Wie wir Ihre Daten verwenden: Wir verwenden Ihre Daten zur Bereitstellung, Unterstützung, Personalisierung und Entwicklung unserer Dienste. Wie wir Ihre personenbezogenen Daten verwenden, hängt davon ab, welche Dienste Sie nutzen, wie Sie diese Dienste nutzen und welche Einstellungen Sie wählen. Wir verwenden Ihre personenbezogenen Daten, um Ihnen, u. a. mithilfe automatisierter Systeme und Schlussfolgerungen unsererseits, unsere Dienste (einschließlich Anzeigen) zur Verfügung zu stellen und diese so anzupassen, dass sie für Sie und andere relevanter und nützlicher sind. Dienste: Mit unseren Diensten können Sie sich mit anderen Personen vernetzen, um Karriere- und Geschäftschancen zu finden bzw. für berufliche Möglichkeiten gefunden zu werden. Unsere Dienste unterstützen Sie dabei, stets informiert zu sein, sich weiterzubilden und produktiver zu werden. Wir verwenden Ihre Daten, um Sie zum Zugriff auf unsere Dienste zu berechtigen, und respektieren Ihre Einstellungen. In Kontakt bleiben: Unsere Dienste ermöglichen es Ihnen, mit Kolleginnen und Kollegen, Partnern, Kunden und anderen beruflichen Kontakten in Verbindung zu bleiben. Dazu können Sie sich mit Fach- und Führungskräften Ihrer Wahl „vernetzen“, die sich auch mit Ihnen „vernetzen“ möchten. Wenn Sie sich mit anderen Mitgliedern vernetzen, können Sie je nach Ihren und deren Einstellungen die Kontakte der anderen Mitglieder durchsuchen, um sich mit ihnen in Bezug auf berufliche Möglichkeiten auszutauschen. Wir verwenden Daten zu Ihrer Person (wie Ihr Profil, Profile, die Sie sich angesehen haben, oder Daten, die über Adressbuch-Uploads oder Partnerintegration bereitgestellt wurden), um es anderen zu ermöglichen, Ihr Profil zu finden, Ihnen und anderen Mitgliedern (beispielsweise Mitgliedern, mit denen Sie Kontakte oder Job Erfahrungen gemein haben), Kontakte vorzuschlagen und es Ihnen zu ermöglichen, andere Personen einzuladen, Mitglied zu werden und sich mit Ihnen zu vernetzen. Sie können außerdem zustimmen, dass wir Ihren genauen Standort oder die Tatsache, dass Sie sich in der Nähe zu anderen Personen befinden, für bestimmte Funktionen verwenden dürfen (z. B. um Ihnen andere Mitglieder in Ihrer Nähe vorzuschlagen, mit denen Sie sich vernetzen können, oder um den Anfahrtsweg zu einem neuen Job zu berechnen oder Ihren Kontakten mitzuteilen, dass Sie sich auf einer beruflichen Veranstaltung befinden). Es bleibt Ihnen überlassen, ob Sie eine andere Person zur Mitgliedschaft bei unseren Diensten einladen, eine Kontaktanfrage senden oder es einem anderen Mitglied gestatten möchten, sich mit Ihnen zu vernetzen. **Wenn Sie eine Person einladen, sich mit Ihnen zu vernetzen, enthält Ihre Einladung Ihre Netzwerkdaten und grundlegende Profildaten (z. B. Ihren Namen, Ihr Profilfoto, Ihre Jobbezeichnung, Ihre Region).** Wir senden Einladungserinnerungen an die von Ihnen eingeladene Person. Sie können entscheiden, ob Sie Ihre eigene Kontaktliste mit Ihren Kontakten teilen möchten oder nicht. Besucher können wählen, wie wir ihre Daten verwenden. Informiert bleiben: Unsere Dienste ermöglichen es Ihnen, über alle Neuigkeiten, Ereignisse und Ideen hinsichtlich beruflicher Themenbereiche, die Ihnen wichtig sind und die von Fachleuten stammen, die Sie respektieren, auf

dem Laufenden zu bleiben. Unsere Dienste ermöglichen es Ihnen auch, Ihr berufliches Wissen zu erweitern und neue Kenntnisse zu erwerben. Wir verwenden die Daten, die uns über Sie vorliegen (z. B. von Ihnen bereitgestellte Daten, Daten, die wir durch Ihre Interaktion mit unseren Diensten erfassen, sowie Schlussfolgerungen, die wir aus den Daten über Sie ziehen), um unsere Dienste für Sie zu personalisieren, indem wir beispielsweise geeignete Inhalte und Diskussionen auf unseren Diensten empfehlen oder nach Relevanz sortieren. Darüber hinaus verwenden wir Ihre personenbezogenen Daten zum Empfehlen von Kenntnissen, die Sie Ihrem Profil hinzufügen könnten oder unter Umständen für Ihre nächsten beruflichen Möglichkeiten ausbauen sollten. Wenn Sie uns daher mitteilen, dass Sie sich für eine neue Kompetenz interessieren (indem Sie sich beispielsweise ein Lernvideo ansehen), verwenden wir diese Informationen, um Inhalte in Ihrem Feed zu personalisieren, vorzuschlagen, dass Sie bestimmten Mitgliedern auf unserer Website folgen oder sich Lerninhalte ansehen, die Ihnen helfen, diese neue Kompetenz zu erwerben. **Wir verwenden Ihre Inhalte, Aktivitäten und andere Daten, einschließlich Ihres Namens und Ihres Fotos, um Mitteilungen an Ihr Netzwerk und andere Personen zu senden.** Je nach Ihren Einstellungen informieren wir möglicherweise andere Personen darüber, dass Sie Ihr Profil aktualisiert, Inhalte veröffentlicht, eine soziale Aktion ausgeführt, eine Funktion verwendet oder einen neuen Kontakt gewonnen haben bzw. dass Sie in den News erwähnt wurden. Karriereseite: Unsere Dienste ermöglichen es Ihnen, Berufswege und Ausbildungsmöglichkeiten zu erforschen, für Karrierechancen gefunden zu werden und Karrierechancen zu entdecken. Personen, die nach neuen Mitarbeiterinnen und Mitarbeitern (für einen Job oder eine spezielle Aufgabe) suchen und auch Personen, die Sie einstellen, können Ihr Profil finden. Wir verwenden Ihre Daten, um Ihnen Jobs oder Mentees zu empfehlen und um Ihnen und anderen relevante berufliche Kontakte zu zeigen (z. B. wer bei einem Unternehmen, in einer Branche, in einem Tätigkeitsbereich oder an einem Standort arbeitet oder über bestimmte Kenntnisse oder Kontakte verfügt). Sie können anzeigen, dass Sie daran interessiert sind, Ihren Job zu wechseln und mit Recruitern Informationen auszutauschen. Wir verwenden Ihre Daten, um Ihnen Jobs zu empfehlen und Sie Recruitern vorzustellen. Wir verwenden möglicherweise automatisierte Systeme, um Inhalte bereitzustellen und Empfehlungen zu geben, damit unsere Dienste für unsere Mitglieder, Besucher und Kunden noch relevanter werden. Wenn Sie Ihr Profil auf dem aktuellen Stand halten, können Sie sich besser mit anderen vernetzen und über unsere Dienste Jobangebote finden. Produktivität: Unsere Dienste ermöglichen es Ihnen, mit Kolleginnen und Kollegen zusammenzuarbeiten, nach potenziellen Klienten, Kunden, Partnern und anderen Personen zu suchen und mit ihnen geschäftlich in Verbindung zu treten. Unsere Dienste ermöglichen es Ihnen, mit anderen Mitgliedern zu kommunizieren und Meetings mit ihnen zu planen und vorzubereiten. Je nach Ihren Einstellungen können wir Nachrichten scannen, um „Bots“ oder ähnliche Tools bereitzustellen, die Aufgaben erleichtern, wie die Planung von Meetings, den Entwurf von Antworten, die Zusammenfassung von Nachrichten oder die Empfehlung nächster Schritte. Premium-Dienste: Mit unseren Premium-Diensten können zahlende Nutzerinnen und Nutzer nach Mitgliedern suchen und mit ihnen Kontakt aufnehmen. Beispiel: Suche nach und Kontaktaufnahme mit Kandidaten für einen Job, Suche nach Neukunden und Mitarbeiterinnen oder Mitarbeitern, Talent-Management und Sponsern von Inhalten über soziale Netzwerke. Wir bieten Premium-Dienste an, die unseren Kunden und Mitgliedern persönlich angepasste Suchfunktionen und Tools (einschließlich Nachrichten- und Aktivitätsmitteilungen) bereitstellen, die Teil unserer Talent Solutions, Marketing Solutions und Sales Solutions sind. Kunden können in begrenztem Umfang Informationen aus Ihrem Profil exportieren, wie den Namen, den Profil-Slogan, das aktuelle Unternehmen, die aktuelle Jobbezeichnung und den allgemeinen Standort (z. B. Dublin), um beispielsweise Vertriebskontakte oder Kandidaten zu verwalten, es sei denn, Sie lehnen dies ab. Im Rahmen dieser Premium-Dienste geben wir keine Kontaktdaten ohne Ihre Einwilligung aus. Ein Premium-Mitglied kann Informationen speichern, die ihm in unseren Premium-Diensten zu Ihrer Person zur Verfügung stehen, wie Lebenslauf, Kontaktdaten oder Verkaufshistorie. Die Daten, die diese Kunden zu Ihrer Person gespeichert haben, unterliegen den Richtlinien der jeweiligen Kunden. Andere Unternehmensdienste und -funktionen, die Ihre Daten verwenden, sind TeamLink und Elevate (Sponsern von Inhalten über Social Media). Kommunikation: Wir kontaktieren Sie und ermöglichen Kommunikation unter Mitgliedern. Wir bieten Einstellungen an, mit denen Sie steuern können, welche Nachrichten und wie oft Sie bestimmte Nachrichtenarten erhalten möchten. **Wir kontaktieren Sie per E-Mail, Telefon, durch auf den LinkedIn Websites oder Apps veröffentlichte Mitteilungen, durch Mitteilungen an Ihr LinkedIn Postfach oder durch andere, im Rahmen der Dienste verfügbare Mittel, einschließlich Textnachrichten (SMS) und Push-Benachrichtigungen.** Wir senden auch Nachrichten in Bezug auf die Nutzung unserer Dienste, Netzwerk-Updates, Erinnerungen, Job-Vorschläge und Werbenachrichten von uns und unseren Partnerunternehmen. Wir senden auch Nachrichten in Bezug auf die Verwendung unserer Dienste, Netzwerk-Updates, Erinnerungen, Job-Vorschläge und Werbenachrichten von uns und unseren **Partnerunternehmen.** Sie können Ihre Kommunikationseinstellungen jederzeit ändern. Bitte beachten Sie, dass Sie den Empfang von Nachrichten zu unseren Diensten nicht ablehnen können. Dazu

gehören Sicherheits- und Rechtshinweise. Wir ermöglichen auch die Kommunikation zwischen Ihnen und anderen Personen durch unsere Dienste, darunter Einladungen, InMail, Gruppen und Nachrichten unter Kontakten. Anzeigen: Wir zeigen Ihnen für Sie angepasste Anzeigen sowohl innerhalb als auch außerhalb unserer Dienste. Sie können wählen, dass Ihnen personalisierte Anzeigen gezeigt werden, aber andere Anzeigen nicht ablehnen. Wir richten Anzeigen (und messen deren Leistung) sowohl innerhalb als auch außerhalb unserer Dienste gezielt an Mitglieder, Besucher und andere Personen, direkt oder über verschiedene Partner. Dazu nutzen wir folgende Daten, entweder kombiniert oder separat: Daten von Anzeigentechnologien sowohl innerhalb als auch außerhalb unserer Dienste, Pixel, Tags, Cookies und Gerätekennungen; Von Mitgliedern bereitgestellte Informationen (beispielsweise Kontaktdaten, Jobbezeichnung und Branche); Daten aus Ihrer Nutzung unserer Dienste (beispielsweise Suchverlauf, Feed, Inhalte, die Sie lesen, wem Sie folgen oder wer Ihnen folgt, Kontakte, Teilnahme an Gruppen, Seitenbesuche, Videos, die Sie sich ansehen, Klicks auf eine Anzeige usw.), einschließlich wie in Abschnitt 1.3 beschrieben; Informationen von Anzeigenpartnern, Anbietern und Herausgebern; und Informationen, die aus den oben aufgeführten Daten abgeleitet werden können (z. B. Nutzung der Jobbezeichnungen eines Profils zur Schlussfolgerung auf eine Branche, Karrierestufe und Vergütungskategorie; Nutzung von Abschlussdaten zur Schlussfolgerung auf das Alter oder Nutzung der Vornamen oder Pronomennutzung zur Schlussfolgerung auf das Geschlecht; Nutzung Ihrer Feed-Aktivitäten zur Schlussfolgerung auf Ihre Interessen oder Nutzung von Gerätedaten, um Sie als Mitglied zu erkennen). Wir zeigen Ihnen Anzeigen mit der Bezeichnung Sponsored Content, die wie ähnliche, nicht gesponserte Inhalte aussehen, mit der Ausnahme, dass sie als Werbung gekennzeichnet sind (z. B. als „Anzeige“ oder „gesponsert“). Wenn Sie bei diesen Anzeigen eine soziale Aktion ausführen (wie „Gefällt mir“, Kommentare oder Teilen), wird Ihre Aktion mit Ihrem Namen verbunden und kann von Dritten gesehen werden. Dazu gehört auch der Anbieter der Werbung. Wenn Sie auf LinkedIn Diensten eine soziale Aktion ausführen (je nach Ihren Einstellungen), kann diese Aktion im Rahmen verbundener Anzeigen genannt werden. Wenn Sie z. B. ein Unternehmen mit „Gefällt mir“ markieren, werden Ihr Name und Foto u. U. angegeben, wenn dessen gesponserte Inhalte angezeigt werden. Anzeigenauswahl: Wir halten uns an die Selbstregulierungsprinzipien für interessenbezogene Werbung und machen von der Option für die Branche Gebrauch, diese Art von Anzeigen abzulehnen. Damit lehnen Sie nicht den Erhalt von Werbung ab. Sie erhalten weiterhin andere Anzeigen von Werbetreibenden, die nicht an diese selbstregulierenden Richtlinien gebunden sind. Sie können auch spezifisch die Verwendung bestimmter Kategorien von Daten durch uns ablehnen, durch die wir Ihnen relevantere Anzeigen präsentieren können. Die Funktion zum Ablehnen für Besucher finden Sie hier. Informationen an Anzeigenanbieter: Wir übermitteln Ihre personenbezogenen Daten nicht an dritte Werbetreibende oder Anzeigennetzwerke, mit folgenden Ausnahmen: (i) gehashte IDs oder Gerätekennungen (soweit diese in einigen Ländern als personenbezogene Daten betrachtet werden); (ii) mit Ihrer separaten Genehmigung (z. B. über ein Formular zur Lead-Generierung) oder (iii) Daten, die bereits jedem Nutzer oder jeder Nutzerin der Dienste zugänglich sind (z. B. Profil). Wenn Sie jedoch eine Anzeige innerhalb oder außerhalb unserer Dienste ansehen oder diese anklicken, wird der Anzeigenbetreiber benachrichtigt, dass jemand die Seite besucht hat, auf der die Anzeige präsentiert wurde, und er kann über Mechanismen wie z. B. Cookies auf Ihre Person schließen. Anzeigenpartner können personenbezogene Daten, die von dem Werbetreibenden direkt von Ihnen erfasst wurden, mit von uns erhaltenen gehashten IDs oder Gerätekennungen in Verbindung bringen. In solchen Fällen versuchen wir, diese Werbepartner vertraglich dazu zu verpflichten, zuvor Ihre ausdrückliche Zustimmung einzuholen. Marketing: Wir empfehlen Ihnen und anderen Personen unsere Dienste. Wir nutzen Mitgliederdaten und -inhalte nicht nur zur Werbung für unsere Dienste, sondern auch für Einladungen und Mitteilungen, um den Ausbau unserer Mitgliederzahlen und unseres Netzwerks, die Interaktion damit und unsere Dienste zu fördern, beispielsweise indem wir Ihren Kontakten zeigen, dass Sie eine Funktion unserer Dienste verwendet haben. Entwicklung unserer Dienste und Forschung: Wir entwickeln unsere Dienste und betreiben Forschung. Entwicklung unserer Dienste: Wir verwenden Daten und Feedback unserer Mitglieder, um Forschung und Entwicklung für unsere Dienste zu betreiben und um Ihnen und anderen Mitgliedern ein besseres, intuitiveres und personalisiertes Erlebnis zu bieten, den Ausbau unserer Mitgliederzahlen und die Interaktion mit unseren Diensten zu fördern, Fach- und Führungskräfte miteinander zu vernetzen und ihnen den Weg zu beruflichen und wirtschaftlichen Chancen zu öffnen. Sonstige Forschung: Wir streben danach, Mitgliedern des globalen Arbeitsmarkts berufliche und wirtschaftliche Chancen zu eröffnen und ihnen zu gesteigerter Produktivität und zu größerem Erfolg zu verhelfen. Wir verwenden die uns zur Verfügung stehenden personenbezogenen Daten, um soziale und wirtschaftliche Trends sowie Entwicklungen auf dem Arbeitsmarkt zu erforschen, wie beispielsweise die Verfügbarkeit von Jobs und Kenntnissen, die für diese Positionen erforderlich sind, sowie Strategien, die dabei helfen, Lücken in verschiedenen Branchen und geografischen Regionen zu schließen. Gelegentlich arbeiten wir im Rahmen dieser Forschung mit vertrauenswürdigen Dritten zusammen und haben Kontrollen

implementiert, die zum Schutz Ihrer Daten vorgesehen sind. Wir veröffentlichen wirtschaftliche Einblicke oder erlauben Dritten die Veröffentlichung solcher Informationen. Diese werden nicht als persönliche, sondern als zusammengefasste Daten präsentiert. Umfragen: Meinungsumfragen werden über unsere Dienste von uns sowie Dritten durchgeführt. Sie sind nicht verpflichtet, auf Umfragen zu antworten und können wählen, welche Informationen Sie mitteilen möchten. Sie können es ablehnen, Einladungen zu Umfragen zu erhalten. Kundensupport: Wir verwenden Daten, um Sie zu unterstützen und Probleme zu beheben. Wir verwenden Daten (möglicherweise auch Nachrichten von Ihnen), um Beschwerden und Problemen mit unseren Diensten nachzugehen, sie anzusprechen und zu beheben (Bugs usw.). Einblicke, die keine Rückschlüsse auf Ihre Person zulassen: Wir verwenden Daten, um Einblicke zu generieren, die keine Rückschlüsse auf Ihre Person zulassen. Wir verwenden Ihre Daten, um Einblicke zu gewinnen und zu teilen. Diese Informationen lassen jedoch keine Rückschlüsse auf Ihre Person zu. Wir verwenden Ihre Daten möglicherweise, um Statistiken über unsere Mitglieder, deren Beruf oder Branche, die Anzahl von bereitgestellten oder angeklickten Ad Impressions oder die demografische Verteilung der Besucher eines Dienstes bzw. demografische Belegschaftseinblicke zu erstellen. Sicherheit und Untersuchungen: Wir verwenden Daten zur Sicherheit, Betrugsprävention und -untersuchung. Wir nutzen Ihre Daten (einschließlich Ihrer Kommunikation) zu Sicherheitszwecken oder zur Untersuchung eines möglichen Betrugs oder anderer Verstöße gegen unsere Nutzervereinbarung und/oder zur Untersuchung eines Versuchs, unseren Mitgliedern, Besuchern oder weiteren Personen Schaden zuzufügen. Zentrale Begriffe : Teilen von Informationen, Unsere Dienste. Alle in Ihrem Profil enthaltenen Informationen und sämtliche Inhalte, die Sie veröffentlichen, oder soziale Aktionen (wie „Gefällt mir“, Kommentare und Teilen), die Sie auf unseren Diensten ausführen, werden in Übereinstimmung mit Ihren Einstellungen von Dritten gesehen. Profil: Ihr Profil ist für alle Mitglieder und Kunden unserer Dienste vollständig sichtbar. Abhängig von Ihren Einstellungen kann es auch für Dritte innerhalb oder außerhalb unserer Dienste sichtbar sein (z. B. für Besucher unserer Dienste oder Nutzer von Drittanbietersuchmaschinen). Wie in unserem Hilfebereich dargelegt, wirken sich Ihre Einstellungen, Ihr Kontaktgrad zu dem Mitglied, das sich Ihr Profil ansieht, dessen Mitgliedschaft und Nutzung unserer Dienste, der Zugangsweg und die Arten der Suche (beispielsweise nach Namen oder Stichwort) auf die Verfügbarkeit Ihres Profils und gewisse Bereiche in Ihrem aus. Beiträge, „Gefällt mir“, Folgen, Kommentare, Nachrichten: Unsere Dienste ermöglichen es Ihnen, Informationen zu lesen und zu teilen. Dazu gehören Beiträge, „Gefällt mir“ und Kommentare und die Funktion „Folgen“. Wenn Sie einen Artikel oder einen Beitrag öffentlich teilen (z. B. ein Update, Bild, Video oder einen Artikel), kann dies von jedem eingesehen und auf jeder Plattform geteilt werden (abhängig von Ihren Einstellungen). Mitglieder, Besucher und Dritte werden Ihre öffentlich geteilten Inhalte einschließlich Ihres Namens (und Fotos, sofern Sie eines bereitgestellt haben) finden und einsehen können. In einer Gruppe sind Beiträge für andere Mitglieder der Gruppe sichtbar. Ihre Mitgliedschaft in Gruppen ist öffentlich und Teil Ihres Profils, jedoch können Sie die Sichtbarkeit in Ihren Einstellungen ändern. Alle Informationen, die Sie über die Seiten von Unternehmen oder anderen Organisationen auf unseren Diensten teilen, können von diesen und anderen Personen gesehen werden, die diese Seiten besuchen. Wenn Sie einer Person oder Organisation folgen, sind Sie für andere Personen und den „Eigentümer“ der Seite als Follower sichtbar. Abhängig von Ihren Einstellungen benachrichtigen wir gegebenenfalls den Absender einer Nachricht, wenn Sie auf seine Nachricht reagieren. Entsprechend Ihrer Einstellungen benachrichtigen wir gegebenenfalls ein Mitglied, wenn Sie sich dessen Profil ansehen. Wenn Sie Inhalte von anderen (auch Anzeigen) mit „Gefällt mir“ markieren, teilen oder kommentieren, können andere diese „sozialen Aktionen“ sehen und Ihnen (d. h. Ihrem Namen, Ihrem Profil und Ihrem Foto, falls vorhanden) zuordnen. Ihr Arbeitgeber kann sehen, wie Sie Dienste und damit verbundene Informationen verwenden, die für Ihre Tätigkeit (beispielsweise als Recruiter oder Vertriebsmitarbeiter) bereitgestellt wurden. Wir zeigen Ihrem Arbeitgeber weder Ihre Jobsuchen noch Ihre persönlichen Nachrichten. Unternehmenskonten: Ihr Arbeitgeber bietet Ihnen möglicherweise Zugriff auf unsere Unternehmensdienste wie Recruiter, Sales Navigator, LinkedIn Learning oder unseren Kampagnen-Manager für Marketing. Er kann Ihre Verwendung dieser Unternehmensdienste überprüfen und verwalten. Abhängig vom Unternehmensdienst fordern wir vor Ihrer Nutzung des betreffenden Dienstes die Genehmigung an, relevante Daten aus Ihrem Profil oder Ihrer Nutzung unserer Dienste für Privatmitglieder mit Ihrem Arbeitgeber teilen zu dürfen. Ein Nutzer von Sales Navigator wird beispielsweise gebeten, seinen „Social Selling Index“ mitzuteilen, eine Punktzahl, die zum Teil auf seinen Aktivitäten innerhalb seines persönlichen Kontos beruht. Wir verstehen, dass bestimmte Aktivitäten, wie die Jobsuche und persönliche Nachrichten, vertraulich sind. Daher teilen wir solche Aktivitäten nicht mit Ihrem Arbeitgeber, es sei denn, Sie haben sich entschieden, sie über unsere Dienste mit Ihrem Arbeitgeber zu teilen (indem Sie sich beispielsweise um eine neue Position bei demselben Unternehmen bewerben oder indem Sie in einer Nachricht an einen Kollegen oder eine Kollegin über unsere Dienste erwähnen, dass Sie auf Jobsuche sind). Wenn Sie Arbeitsplatz-Tools und -dienste verwenden (z. B. interaktive Mitarbeiterverzeichnis-Tools), werden abhängig von Ihren

Einstellungen bestimmte Ihrer Daten möglicherweise auch Ihrem Arbeitgeber zur Verfügung gestellt oder mit Informationen verknüpft, die wir von Ihrem Arbeitgeber erhalten, um diese Tools und Dienste zu ermöglichen. Kommunikationsarchivierung: Mitglieder, die in einem regulierten Umfeld tätig sind, müssen Mitteilungen möglicherweise außerhalb unserer Dienste speichern. Manche Mitglieder (oder deren Arbeitgeber) müssen ihre Mitteilungen und Aktivitäten auf sozialen Netzwerken aus Gründen der Einhaltung rechtlicher oder beruflicher Vorgaben möglicherweise archivieren und nutzen dafür die Dienste Dritter, die ihnen diese Archivierungsdienste bereitstellen. Wir ermöglichen die Archivierung von Mitteilungen durch und für solche Mitglieder außerhalb unserer Dienste. Ein Beispiel dafür wäre ein Finanzberater, der Kommunikationen mit seinem Klienten im Rahmen seiner Zulassung als Finanzberater über unsere Dienste archivieren muss. Dienste Dritter: Sie können Ihr Konto mit den Diensten Dritter verknüpfen, sodass diese die Profile Ihrer Kontakte aufrufen, von Ihnen geteilte Beiträge auf ihren Plattformen posten oder es Ihnen ermöglichen können, mit Ihren Kontakten auf ihren Plattformen zu kommunizieren. Außerdem erscheinen Auszüge Ihres Profils auf den Diensten Dritter. Abhängig von Ihren Einstellungen können andere Dienste Ihr Profil aufrufen. Wenn Sie sich entscheiden, Ihr Konto mit einem anderen Dienst zu verknüpfen, hat dieser Zugang zu Ihren persönlichen Daten. Wenn Sie die Konten verknüpfen, finden Sie eine Beschreibung, wie Ihre personenbezogenen Daten geteilt und verwendet werden, auf einem Einwilligungsbildschirm oder über einen Link, wo Sie Ihre Einwilligung dazu geben. Sie können Ihr Twitter oder WeChat Konto beispielsweise verbinden, um Inhalte von unseren Diensten auf diesen anderen Diensten zu teilen, oder Ihr E-Mail-Anbieter gibt Ihnen vielleicht die Möglichkeit, Ihre LinkedIn Kontakte auf seinen eigenen Dienst hochzuladen. Dienste Dritter unterliegen ihren eigenen Datenschutzrichtlinien. Sie könnten dem Betreiber die Nutzung Ihrer Daten in einer Art und Weise einräumen, die von unseren Gepflogenheiten abweicht. Sie können die Verknüpfung mit solchen Konten aufheben. **Abhängig von Ihren Einstellungen erscheinen Auszüge aus Ihrem Profil auf den Diensten Dritter (beispielsweise Suchmaschinen-Ergebnisse, E-Mail- und Kalender-Apps, die eingeschränkte Profildaten der Person anzeigen, der eine Nachricht oder SMS gesendet wird, soziale Medien-Aggregatoren, Talent- und Lead-Manager).** „Alte“ Profilinformationen bleiben weiterhin auf diesen Diensten bestehen, bis diese ihren Daten-Cachespeicher mit den von Ihnen vorgenommenen Profiländerungen aktualisieren. Ähnliche Dienste: Wir teilen Ihre Daten über unsere verschiedenen Dienste und mit LinkedIn verbundenen Unternehmen. Wir teilen Ihre personenbezogenen Daten mit den mit uns verbundenen Unternehmen, um unsere Dienste bereitzustellen und weiterzuentwickeln. Wir führen unter Umständen Daten intern über verschiedene in dieser Datenschutzrichtlinie erfasste Dienste zusammen, um unsere Dienste für Sie und andere relevanter und nützlicher zu gestalten. Wir können beispielsweise Ihren Feed oder Ihre Jobempfehlungen basierend auf Ihrem Lernverlauf personalisieren. Dienstleister: Möglicherweise nutzen wir die Dienste Dritter zur Unterstützung unserer Dienste. Wir nutzen die Dienste Dritter, um uns bei der Bereitstellung unserer Dienste zu unterstützen (beispielsweise Wartung, Analyse, Prüfung, Zahlung, Betrugserkennung, Marketing und Entwicklung). Diese Dritten haben in dem Ausmaß Zugang zu Ihren Informationen wie angemessen erforderlich, um die betreffenden Aufgaben für uns zu erledigen, und sind verpflichtet, Ihre Informationen nicht offenzulegen oder für andere Zwecke zu nutzen. Gesetzliche Offenlegung: Möglicherweise ist es erforderlich, Ihre Daten zu teilen, wenn dies unserer Ansicht nach gesetzlich nötig ist, um Ihre oder unsere Rechte und Sicherheit oder die Dritter zu schützen. Unter Umständen müssen wir Ihre Informationen offenlegen, wenn dies gesetzlich, aufgrund einer Vorladung oder aus anderen rechtlichen Gründen erforderlich ist, oder wenn wir in gutem Glauben davon ausgehen können, dass die Offenlegung angemessenerweise erforderlich ist, um (1) mutmaßliche oder tatsächliche illegale Vorgänge zu untersuchen, zu verhindern oder entsprechende Maßnahmen zu ergreifen oder um staatliche Vollzugsbehörden zu unterstützen, um (2) unsere Vereinbarungen mit Ihnen durchzusetzen, (3) den Forderungen und Beschuldigungen Dritter nachzugehen und uns dagegen zu verteidigen, (4) die Sicherheit und Integrität unserer Dienste zu schützen (indem wir Informationen beispielsweise mit Unternehmen teilen, die auf ähnliche Weise bedroht sind), oder um (5) Rechte geltend zu machen und die Rechte und Sicherheit von LinkedIn, unseren Mitgliedern, Mitarbeiterinnen und Mitarbeitern und Dritten zu schützen. Wir versuchen, Mitglieder über rechtliche Anforderungen ihrer personenbezogenen Daten zu informieren, sofern dies unseres Erachtens angemessen ist, es sei denn, dies ist gesetzlich oder aufgrund einer gerichtlichen Anordnung verboten, oder es handelt sich bei der Anforderung um einen Notfall. Wir können derartige Anforderungen anfechten, wenn wir nach unserem Ermessen der Ansicht sind, dass die Anforderungen zu allgemein oder vage sind oder wenn es sich um mangelnde Befugnis handelt, verpflichten uns jedoch nicht, alle Anforderungen anzufechten. Weiteres erfahren Sie in unseren Richtlinien für die Anforderung von Daten in unserem Transparenzbericht. Kontrollwechsel oder Verkauf: Wir teilen Ihre Daten möglicherweise, wenn unser Unternehmen an Dritte verkauft wird. Sie müssen jedoch weiterhin in Übereinstimmung mit dieser Datenschutzrichtlinie verwendet werden. Wir können Ihre Daten auch im Rahmen eines Verkaufs, einer Fusion oder eines Kontrollwechsels oder in

Vorbereitung auf eines dieser Ereignisse teilen. Ein anderes Unternehmen, das uns oder einen Teil unseres Unternehmens kauft, hat das Recht, Ihre Daten zu verwenden, jedoch nur auf die in dieser Datenschutzrichtlinie dargelegte Art und Weise, es sei denn, Sie vereinbaren etwas anderes. Ihre Optionen und Verpflichtungen, Aufbewahrung von Daten: Wir behalten die meisten Ihrer personenbezogenen Daten so lange, wie Sie ein aktives Konto auf LinkedIn haben.

Generell bewahren wir Ihre personenbezogenen Daten so lange auf, wie Ihr Konto aktiv ist oder wie es erforderlich ist, um Ihnen Dienste bereitzustellen. Darunter fallen Daten, die Sie oder andere uns zur Verfügung stellen sowie Daten, die durch die Nutzung unserer Dienste generiert oder abgeleitet wurden. Auch wenn Sie unsere Dienste nur nutzen, wenn Sie alle paar Jahre einen neuen Job suchen, bewahren wir Ihre Informationen auf und Ihr Profil bleibt aktiv, es sei denn, Sie schließen Ihr Konto. Wir behalten uns vor, in einigen Fällen bestimmte Informationen (z. B. Einblicke über die Nutzung der Dienste) in entpersonalisierter oder aggregierter Form aufzubewahren. Recht auf Zugriff auf und Kontrolle Ihrer personenbezogenen Daten: Sie können auf Ihre personenbezogenen Daten zugreifen oder sie löschen. Sie haben viele Optionen und können wählen, wie Ihre Daten erfasst, verwendet und geteilt werden. Wir bieten Ihnen viele Optionen bezüglich des Erfassens, Verwendens und Teilens Ihrer Daten, angefangen beim Löschen oder Korrigieren der Daten, die Sie in Ihrem Profil angeben, und der Kontrolle über die Sichtbarkeit Ihrer Beiträge, bis hin zum Ablehnen von Werbung und Verwalten von Nachrichten. Sie haben die Möglichkeit, Einstellungen bezüglich der Daten vorzunehmen, die uns zu Ihrer Person vorliegen. In Bezug auf Daten, die uns zu Ihrer Person vorliegen, können Sie: Daten löschen: Sie können von uns die Löschung Ihrer gesamten personenbezogenen Daten oder eines Teils davon verlangen (wenn beispielsweise die Erbringung von Dienstleistungen für Sie nicht mehr erforderlich ist). Daten ändern oder berichtigen: Sie können einige Ihrer personenbezogenen Daten über Ihr Konto bearbeiten. Sie können uns auch in bestimmten Fällen um die Änderung, Aktualisierung oder Korrektur Ihrer Daten bitten, insbesondere, wenn diese fehlerhaft sind. Die Nutzung von Daten beanstanden oder einschränken: Sie können von uns verlangen, die Nutzung Ihrer personenbezogenen Daten ganz oder zum Teil einzustellen (wenn wir beispielsweise keine rechtliche Grundlage für ihre weitere Nutzung haben), oder die Nutzung einzuschränken (wenn beispielsweise Ihre personenbezogenen Daten unzutreffend sind oder rechtswidrig von uns beibehalten werden). Recht auf Zugriff bzw. Abbild Ihrer Daten: Sie können von uns eine Kopie Ihrer personenbezogenen Daten verlangen, und Sie können eine Kopie der von Ihnen überlassenen personenbezogenen Daten in maschinenlesbarer Form verlangen. Besucher erfahren hier mehr darüber, wie sie eine solche Anfrage stellen können. Sie können sich über die unten stehenden Kontaktinformationen an uns wenden. Wir werden Ihre Anfrage den gültigen Gesetzen entsprechend prüfen. Personen mit Wohnsitz in einem der designierten Länder und anderen Regionen haben möglicherweise weitere gesetzlich vorgeschriebene Rechte. Kontoschließung: Wir behalten einige Ihrer Daten, auch nachdem Sie Ihr Konto geschlossen haben. Wenn Sie Ihr LinkedIn-Konto schließen, sind Ihre personenbezogenen Daten in der Regel innerhalb von 24 Stunden nicht mehr für andere Personen auf unseren Diensten sichtbar. Generell löschen wir die Informationen in einem geschlossenen Konto innerhalb von 30 Tagen nach der Kontoschließung, außer wie unten angegeben. Wir bewahren Ihre personenbezogenen Daten auch nach der Schließung Ihres Kontos auf, wenn dies angemessen und erforderlich ist, um unseren rechtlichen Pflichten (einschließlich Anforderungen durch Strafverfolgungsbehörden) nachzukommen, regulatorische Vorgaben einzuhalten, Streitsachen zu schlichten, für Sicherheit zu sorgen, Betrug und Missbrauch vorzubeugen (beispielsweise, wenn wir Ihr Konto wegen einer Verletzung unserer Community-Richtlinien eingeschränkt haben), unsere Nutzervereinbarung durchzusetzen oder Ihrer Abbestellung weiterer Mitteilungen von uns zu entsprechen. Nach der Schließung Ihres Kontos bewahren wir entpersonalisierte Daten weiter auf. Informationen, die Sie mit Dritten geteilt haben (beispielsweise per InMail, in Updates oder Beiträgen zu Gruppen), bleiben sichtbar, nachdem Sie Ihr Konto geschlossen oder die Informationen aus Ihrem eigenen Profil oder Ihrem Postfach gelöscht haben. Des Weiteren kontrollieren wir keine Daten, die andere Mitglieder aus unseren Diensten kopiert haben. Bei Gruppeninhalten und Bewertungen oder Inhalten zur Prüfung von geschlossenen Konten wird als Quelle „unbekannter Nutzer“ angezeigt. Möglicherweise wird Ihr Profil weiterhin auf den Diensten Dritter angezeigt (beispielsweise in Suchmaschinenergebnissen), bis diese ihren Cache-Speicher aktualisiert haben. Weitere wichtige Informationen: Sicherheit: Wir prüfen, ob gegen unsere Sicherheit verstoßen wird und versuchen, derartige Verstöße zu verhindern. Bitte nutzen Sie die in unseren Diensten verfügbaren Sicherheitsfunktionen. Wir implementieren Sicherheitsschutzmaßnahmen, wie HTTPS, die zum Schutz Ihrer Daten vorgesehen sind. Wir prüfen unsere Systeme regelmäßig auf mögliche Schwachstellen und Angriffe. Wir können die Sicherheit der uns von Ihnen übermittelten Informationen jedoch nicht gewährleisten. Es gibt keine Garantie dafür, dass nicht auf Daten zugegriffen wird oder dass diese nicht offengelegt, geändert oder infolge der Verletzung unserer physischen, technischen und organisatorischen Sicherheitsvorkehrungen zerstört werden. Weitere Informationen über die sichere Nutzung unserer Dienste, einschließlich der zweistufigen

Authentifizierung, finden Sie in unserem Sicherheitsbereich. Landesübergreifender Datentransfer: Wir speichern und nutzen Ihre Daten außerhalb Ihres Landes. Wir verarbeiten Daten sowohl innerhalb als auch außerhalb der USA und bedienen uns dabei gesetzlich vorgesehener Mechanismen für die rechtmäßige grenzübergreifende Übertragung von Daten. Mehr dazu. Möglicherweise gelten in den Ländern, in denen wir Daten verarbeiten, andere Gesetze, die eventuell nicht denselben Grad an Schutz bieten wie die Gesetze in Ihrem Land. Rechtsgrundlage für die Verarbeitung: Die Erfassung, Verwendung und Weitergabe der Daten, die uns zu Ihrer Person vorliegen, erfolgt auf rechtlicher Grundlage. Bezüglich der Verwendung Ihrer Daten haben Sie Wahlmöglichkeiten. Über Ihre Einstellungen können Sie jederzeit Ihre Einwilligung widerrufen. Wir erfassen und verarbeiten personenbezogene Daten über Sie nur, wenn dafür eine entsprechende Rechtsgrundlage besteht. Als Rechtsgrundlage gelten unter anderem Einwilligung (wenn Sie Ihre Einwilligung gegeben haben), Vertrag (wenn die Verarbeitung für die Erfüllung eines Vertrags mit Ihnen – beispielsweise die Erbringung der von Ihnen verlangten LinkedIn Dienste – erforderlich ist) und „legitime Interessen“. Wenn wir uns bei der Verarbeitung personenbezogener Daten auf Ihre Einwilligung berufen, sind Sie berechtigt, Ihre Einwilligung jederzeit zurückzuziehen oder zu verweigern. Wenn wir uns auf legitime Interessen berufen, sind Sie berechtigt, Einspruch dagegen zu erheben. Mehr dazu. Wenn Sie Fragen zur Rechtsgrundlage haben, auf der wir Ihre personenbezogenen Daten erfassen und verwenden, wenden Sie sich bitte hier an unseren Datenschutzbeauftragten. Direktmarketing und „Do Not Track“-Signale: Unsere Aussagen zu Direktmarketing und „Do Not Track“-Signalen. Ohne Ihre Erlaubnis geben wir keine personenbezogenen Daten an Dritte für deren Direkt-Marketing-Zwecke weiter. Erfahren Sie mehr über dieses Thema und über unsere Haltung gegenüber „Do Not Track“-Signalen. Kontaktinformationen: Sie können sich mit uns in Verbindung setzen oder andere Optionen nutzen, um Beschwerden beizulegen. Sollten Sie Fragen oder Beschwerden hinsichtlich dieser Richtlinie haben, kontaktieren Sie LinkedIn bitte zuerst online. Sie können uns auch auf dem Postweg erreichen. Wenn Ihre Beschwerde nicht durch eine Kontaktaufnahme mit uns beigelegt werden konnte, haben Sie weitere Möglichkeiten. Personen mit Wohnsitz in einem der „designierten Länder“ und anderen Regionen haben möglicherweise auch das Recht, unseren Datenschutzbeauftragten hier zu kontaktieren. Wenn Ihre Beschwerde dadurch nicht beigelegt werden kann, haben Personen mit Wohnsitz in einem der „designierten Länder“ und anderen Regionen möglicherweise im Rahmen ihrer Gesetze weitere Möglichkeiten.

Einleitung

Diese Datenschutzerklärung („Datenschutzerklärung“) gilt für die Verarbeitung von personenbezogenen Daten durch TikTok im Zusammenhang mit den Anwendungen, den Webseiten, der Software und den zugehörigen Diensten von TikTok (die „Plattform“), die auf diese Datenschutzerklärung verlinken oder darauf verweisen. Datenverantwortlicher: Wenn Sie im Europäischen Wirtschaftsraum („EWR“), im Vereinigten Königreich („UK“) oder in der Schweiz leben, sind TikTok Technology Limited, ein irisches Unternehmen („TikTok Irland“), und TikTok Information Technologies UK Limited („TikTok UK“), ein britisches Unternehmen („TikTok“, „unser“, „wir“ oder „uns“) die gemeinsamen Verantwortlichen für die Verarbeitung Ihrer Daten im Zusammenhang mit dieser Datenschutzerklärung. Welche personenbezogenen Daten wir erheben: Wir erheben drei Kategorien von Daten: Von Ihnen bereitgestellte Daten, automatisch erhobene Daten und Daten aus anderen Quellen. Weitere Einzelheiten finden Sie unten. Von Ihnen bereitgestellte Daten: Profilinformationen. Wir erheben Daten, die Sie bei der Einrichtung eines Kontos angeben, wie z. B. Ihr Geburtsdatum, Ihren Benutzernamen, Ihre E-Mail-Adresse und/oder Telefonnummer und Ihr Passwort. Sie können Ihrem Profil weitere Informationen hinzufügen, wie z. B. eine Beschreibung oder ein Profilfoto. Nutzerinhalte: Wir erheben die von Ihnen erstellten oder über die Plattform veröffentlichten Inhalte, wie z. B. Fotos, Videos, Audioaufnahmen, Livestreams und Kommentare, sowie die zugehörigen Metadaten (z. B. wann, wo und von wem die Inhalte erstellt wurden). Auch wenn Sie kein Nutzer sind, können Informationen über Sie in Inhalten erscheinen, die von Nutzern auf der Plattform erstellt oder veröffentlicht werden. Wir erheben Nutzerinhalte durch Vorabladen zum Zeitpunkt der Erstellung, des Imports oder des Hochladens, unabhängig davon, ob Sie diese Nutzerinhalte speichern oder hochladen, z. B. um Musik auf der Grundlage des Videos zu empfehlen. Wir erheben auch Inhalte (z. B. Text, Bilder und Videos) aus der Zwischenablage Ihres Geräts, wenn Sie Inhalte auf die Plattform kopieren und einfügen oder Inhalte zwischen der Plattform und einer Drittanbieterplattform austauschen. Darüber hinaus erheben wir Standortinformationen (wie z. B. Sehenswürdigkeiten, Shops oder andere Points of Interest), wenn Sie sich dafür entscheiden, die Standortinformationen zu Ihren Nutzerinhalten hinzuzufügen. Direktnachrichten. Wenn Sie mit anderen über Direktnachrichten kommunizieren, erheben wir den Inhalt der Nachricht und die zugehörigen Metadaten (z. B. den Zeitpunkt, zu dem die Nachricht gesendet, empfangen und/oder gelesen wurde, sowie die Teilnehmer der Kommunikation). Wir tun dies, um Spam zu blockieren, Straftaten aufzudecken und unsere Nutzer zu schützen. Ihre Kontakte: Wenn Sie sich dafür entscheiden, Ihre Kontakte zu importieren, erheben wir Daten aus dem Telefonbuch Ihres Geräts oder aus Ihren Kontakten in sozialen Medien. Wir verwenden diese Daten, um Ihnen beim Knüpfen von Kontakten zu helfen, z. B. wenn Sie unsere Funktion „Freunde finden“ nutzen, und um Ihnen Konten vorzuschlagen. Kaufinformationen: Wir erheben Ihre Zahlungskartendaten oder andere Zahlungsdaten von Drittanbietern (wie PayPal), wenn eine Zahlung erforderlich ist. Außerdem erheben wir Ihren Transaktions- und Kaufverlauf. Umfragen, Forschung und Werbeaktionen. Wir erheben Daten, die Sie uns zur Verfügung stellen, wenn Sie sich für die Teilnahme an einer Umfrage, einer Forschung, einer Werbeaktion, einem Wettbewerb, einer Marketingkampagne oder einer von uns durchgeführten oder gesponserten Veranstaltung entscheiden. Informationen, wenn Sie uns kontaktieren: Wenn Sie mit uns in Kontakt treten, erheben wir die Daten, die Sie uns senden, wie z. B. Identitäts- oder Altersnachweise, Feedback oder Anfragen zu Ihrer Nutzung der Plattform oder Informationen über mögliche Verstöße gegen unsere Nutzungsbedingungen (unsere „Nutzungsbedingungen“), Community-Richtlinien (unsere „Richtlinien“) oder andere Bestimmungen. Automatisch erhobene Daten: Technische Daten: Wir erheben bestimmte Geräte- und Netzwerkverbindungsdaten, wenn Sie auf die Plattform zugreifen. Zu diesen Daten gehören Ihr Gerätemodell, Ihr Betriebssystem, Tastenanschlagmuster oder -rhythmen, Ihre IP-Adresse und Ihre Systemsprache. Wir erheben auch dienstbezogene, diagnostische und Leistungsdaten, einschließlich Absturzberichte und Leistungsprotokolle. Wir weisen Ihnen automatisch eine Geräte-ID und eine Nutzer-ID zu. Wenn Sie sich von mehreren Geräten aus anmelden, verwenden wir Daten wie Ihre Geräte-ID und Ihre Nutzer-ID, um Ihre Aktivitäten geräteübergreifend zu identifizieren, um Ihnen ein nahtloses Anmeldeerlebnis zu bieten sowie aus Sicherheitsgründen. Standortinformationen: Wir erheben automatisch Informationen über Ihren ungefähren Standort (z. B. Land, Bundesland oder Stadt) auf der Grundlage Ihrer technischen Daten (z. B. SIM-Karte und IP-Adresse). Wenn Sie in den Einstellungen Ihres Geräts Standortdienste für die TikTok-App aktivieren, erheben wir außerdem ungefähre Standortinformationen von Ihrem Gerät. Klicken Sie hier, um mehr darüber zu erfahren, wie wir Standortinformationen erheben. Informationen über die Nutzung: Wir erheben Daten darüber, wie Sie unsere Plattform nutzen, einschließlich Daten über die von Ihnen angesehenen Inhalte, die Dauer und Häufigkeit Ihrer Nutzung, wie Sie mit anderen Nutzern in Kontakt treten, Ihren Suchverlauf und

Ihre Einstellungen. Inhaltliche Merkmale und Eigenschaften: Wir erkennen und erheben Merkmale und Eigenschaften der Video- und Audioaufnahmen, die Teil Ihrer Nutzerinhalte sind, z. B. durch die Identifizierung von Objekten und Landschaften, das Vorhandensein oder die Position eines Gesichts oder anderer Körperteile innerhalb eines Bildes und den Text der in Ihren Nutzerinhalten gesprochenen Wörter. Wir tun dies zum Beispiel für die Moderation von Inhalten und zur Bereitstellung von Spezialeffekten (wie Videofilter und Avatare) und Untertiteln.

Hergeleitete Daten: Wir schließen von den Daten, die wir über Sie vorliegen haben, auf Ihre Eigenschaften (z. B. Altersgruppe und Geschlecht) und Interessen. Wir verwenden diese Rückschlüsse zum Beispiel, um unsere Plattform sicher zu halten, um Inhalte zu moderieren und, sofern zulässig, um Ihnen personalisierte Werbung auf der Grundlage Ihrer Interessen bereitzustellen.

Cookies: Wir verwenden Cookies und ähnliche Tracking-Technologien für den Betrieb und die Bereitstellung unserer Dienste. Wir verwenden Cookies beispielsweise, um Ihre Spracheinstellungen zu speichern, um sicherzustellen, dass Sie dasselbe Video nicht mehr als einmal sehen, und aus Sicherheitsgründen. Wir verwenden diese Technologien auch für Marketingzwecke. Weitere Informationen über unsere Verwendung von Cookies finden Sie in unserer Cookie-Richtlinie für die TikTok-Webseiten und unserer Cookie-Richtlinie für die TikTok-Plattform. Wo dies gesetzlich vorgeschrieben ist, holen wir Ihr Einverständnis zur Verwendung von Cookies ein. Daten aus anderen Quellen: Werbe-, Mess- und Datenpartner. Werbe-, Mess- und Datenpartner teilen mit uns Daten wie mobile Identifikatoren für Werbung, gehashte E-Mail-Adressen und Ereignisdaten über die Aktionen, die Sie auf einer Website oder App durchgeführt haben. Einige unserer Werbekunden und andere Partner ermöglichen es uns, ähnliche Daten direkt von ihrer Website oder App zu erheben, indem sie unsere TikTok Advertiser Tools (wie TikTok Pixel) integrieren. Plattformen und Partner von Drittanbietern: Wenn Sie sich auf der Plattform anmelden oder sich über die von diesen Drittanbietern bereitgestellten Anmeldefunktionen einloggen, stellen uns Plattformen von Drittanbietern Daten zur Verfügung (z. B. Ihre E-Mail-Adresse, Ihre Nutzer-ID und Ihr öffentliches Profil). Wir können auch Kontaktinformationen erhalten, die Sie besitzen oder die über Sie gespeichert sind, wenn Kontaktinformationen von Ihnen oder einem anderen Nutzer mit unserer Plattform synchronisiert werden. Wenn Sie mit einem Dienst eines Drittanbieters (z. B. Apps, Webseiten oder Produkte von Drittanbietern) interagieren, der TikTok Developer Tools integriert, erhalten wir die Daten, die erforderlich sind, um Ihnen Funktionen wie dienstübergreifende Authentifizierung oder Cross-Posting zur Verfügung zu stellen. Dies geschieht beispielsweise, wenn Sie sich mit Ihrem TikTok-Konto bei einer anderen Plattform anmelden oder wenn Sie die TikTok-Schaltfläche „Teilen“ auf einer Plattform eines Drittanbieters verwenden, um Inhalte von dort auf der Plattform zu teilen. Andere: Wir können Daten über Sie von anderen erhalten, z. B. wenn Sie in Nutzerinhalten, Direktnachrichten, einer Beschwerde, einem Einspruch, einer Anfrage oder einem Feedback, das von einem Nutzer oder einem Dritten eingereicht wurde, enthalten sind oder erwähnt werden, oder wenn uns ein Nutzer Ihre Kontaktinformationen zur Verfügung stellt. Wie wir Ihre personenbezogenen Daten verwenden: Wir verwenden Ihre Daten, um unsere Dienste zu betreiben, bereitzustellen, weiterzuentwickeln und zu verbessern, unter anderem für die folgenden Zwecke. Weitere Einzelheiten finden Sie unter „Unsere Rechtsgrundlagen und wie wir Ihre personenbezogenen Daten verarbeiten“. Bereitstellung und Verwaltung unserer Dienste, z. B. um Ihnen die Möglichkeit zu geben, Inhalte zu erstellen, zu teilen und zu konsumieren und mit anderen Nutzern und deren Inhalten zu interagieren. Personalisierung und Anpassung Ihrer Erfahrung auf der Plattform, wie z. B. die Bereitstellung Ihres „Für dich“-Feeds. Bearbeitung, Vermittlung oder Erfüllung von Anfragen zum Kauf von Produkten, Waren und Dienstleistungen. Durchsetzung unserer Nutzungsbedingungen, Richtlinien und anderer für Sie geltender Bestimmungen. Wir überprüfen Nutzerinhalte und andere Daten, um die Sicherheit und das Wohlergehen unserer Community zu schützen. Bereitstellung bestimmter interaktiver Funktionen, wie z. B. die Möglichkeit, Ihre Inhalte in den Videos anderer Nutzer zu verwenden und anderen Nutzern Ihr Konto vorzuschlagen, um Sie mit anderen Nutzern in Verbindung zu bringen. Bereitstellung und Verbesserung unserer Werbedienste, einschließlich der Schaltung von Anzeigen (einschließlich personalisierter Anzeigen, sofern zulässig) und der Messung und des Verständnisses der Wirksamkeit der Anzeigen und anderer Inhalte. Aufrechterhaltung und Verbesserung der Sicherheit und Stabilität unserer Dienste durch die Identifizierung und Behebung von technischen oder sicherheitsrelevanten Problemen (z. B. technische Bugs, Spam-Konten, Aufdeckung von Missbrauch, Betrug und illegalen Aktivitäten). Überprüfung, Verbesserung und Weiterentwicklung der Plattform, u. a. durch Überwachung der Interaktionen und der Nutzung über Ihre Geräte hinweg, durch Analyse der Nutzung der Plattform durch die Nutzer und durch die Schulung und Verbesserung unserer Technologie, wie z. B. unserer maschinellen Lernmodelle und Algorithmen. Teilen Ihrer Informationen mit Plattformen von Drittanbietern, um Ihnen Funktionen zur Verfügung zu stellen, wie z. B. das Teilen von Inhalten auf Ihren Wunsch, wenn Sie Ihr TikTok-Konto mit einem Dienst eines Drittanbieters verbinden. Bewerbung der Plattform oder der Dienste Dritter durch Marketingmitteilungen, Wettbewerbe oder Werbeaktionen. Erfüllung unserer rechtlichen Verpflichtungen oder zur Erfüllung von Aufgaben, die im

öffentlichen Interesse liegen, oder zum Schutz der lebenswichtigen Interessen unserer Nutzer und anderer Personen. **Wie wir Ihre personenbezogenen Daten weitergeben. Dienstanbieter:** Wir beauftragen Dienstanbieter, die uns helfen, unsere Dienste bereitzustellen, zu unterstützen und weiterzuentwickeln und zu verstehen, wie sie genutzt werden. Sie bieten Dienstleistungen wie Cloud-Hosting, Bereitstellung von Inhalten, Kunden- und technischen Support, Inhaltsmoderation, Marketing, Analysen und Online-Zahlungen an. **Wir geben die von Ihnen bereitgestellte Daten, automatisch erhobenen Daten und Daten aus anderen Quellen an diese Dienstleister weiter, soweit dies erforderlich ist, damit diese ihre Dienste erbringen können.** **Partner:** Plattformen und Partner von Drittanbietern. **Wir teilen begrenzte Informationen, zu denen die von Ihnen bereitgestellten Daten, technischen Daten und Informationen über die Nutzung gehören können, mit Drittplattformen und Partnern, deren Plattform oder Dienste in die Plattform integriert sind.** Wir tun dies, um Ihnen ein nahtloses Erlebnis zu bieten und Ihnen zu ermöglichen, dass Ihre Inhalte auf anderen Plattformen geteilt werden können, und/oder um Plattformen und Partnern von Drittanbietern eine bessere Authentifizierung der Nutzer zu ermöglichen. Zum Beispiel, wenn Sie sich entscheiden: sich mit Ihrem TikTok-Konto bei einer Plattform eines Drittanbieters anzumelden, werden wir Ihre grundlegenden Kontoinformationen und alle anderen von Ihnen bereitgestellten Daten weitergeben; sich mit Ihren Kontodaten von einer Drittplattform (z. B. Facebook oder Google) bei der Plattform anzumelden oder einzuloggen, werden wir bestimmte technische Daten weitergeben, um dies zu ermöglichen; Nutzerinhalte, die Sie auf der Plattform veröffentlichen, auf anderen Social-Media-Plattformen zu teilen, werden wir Ihre Nutzerinhalte und damit verbundene Daten weitergeben. **Werbepartner:** Wir stellen Werbetreibenden zusammengefasste Daten über die Leistung ihrer Anzeigen und anderer Inhalte auf der Plattform zur Verfügung, um ihnen zu helfen, ihre Wirksamkeit zu messen. Wir erstellen diese zusammengefassten Daten mithilfe von von Ihnen bereitgestellten Daten, automatisch erhobenen Daten und Daten aus anderen Quellen. Wir geben Ihre Daten direkt an Werbetreibende weiter, wenn Sie uns dazu Ihre Erlaubnis erteilen. **Mess- und Datenpartner:** **Wir geben Ihre technischen Daten und Informationen über die Nutzung auch an Drittanbieter weiter, die uns dabei helfen, die Werbung auf unserer Plattform zu messen und unseren Werbetreibenden dabei zu helfen, die Wirksamkeit ihrer Werbung zu ermitteln.** **Unsere Unternehmensgruppe:** Als globales Unternehmen wird die Plattform von bestimmten Unternehmen innerhalb unserer Unternehmensgruppe („Unternehmensgruppe“) unterstützt. Diese Unternehmen verarbeiten die von Ihnen bereitgestellten Daten, automatisch erhobenen Daten und Daten aus anderen Quellen für uns, soweit dies erforderlich ist, damit wichtige Funktionen wie Speicherung, Bereitstellung von Inhalten, Sicherheit, Forschung und Entwicklung, Analysen, Online-Zahlungen, Kunden- und technischer Support sowie die Moderation von Inhalten bereitgestellt werden können. Siehe „Unsere globalen Aktivitäten und Datenübertragungen“ für weitere Informationen. **Andere:** Wir geben Ihre Daten in anderen begrenzten Szenarien wie folgt weiter: **Andere Nutzer und die Öffentlichkeit.** Je nach Ihren Datenschutzeinstellungen können Ihre Profilinformationen und Ihre Nutzerinhalte für andere Nutzer und die Öffentlichkeit sichtbar sein. Hier erfahren Sie mehr über Kontotypen und Datenschutzeinstellungen, einschließlich darüber, wie Sie das Publikum für Ihre Videos einschränken können. Ihr Profil und Ihre Inhalte können auch für Dritte sichtbar sein, z. B. für Suchmaschinen, Inhalteaggregatoren und Nachrichtenseiten. Sie und andere Personen können Ihre Nutzerinhalte sowohl auf der Plattform als auch außerhalb der Plattform weitergeben, je nachdem, was Sie in Ihren Datenschutzeinstellungen festgelegt haben. **Nutzer unserer Analysedienste.** Wir stellen aggregierte Statistiken und Einblicke zur Verfügung, um Menschen und Unternehmen dabei zu helfen, zu verstehen, wie mit der Plattform interagiert wird. So können Creator*innen und Werbetreibende beispielsweise Informationen über die Anzahl der Aufrufe, Likes, Kommentare und Freigaben ihrer Videos sowie demografische Informationen über ihre Follower und die Betrachter ihrer Videos erhalten. Wir erstellen diese zusammengefassten Daten mithilfe von von Ihnen bereitgestellten Daten und automatisch erhobenen Daten. **Unternehmenstransaktionen:** Ihre Daten können im Zusammenhang mit einer Unternehmenstransaktion wie z. B. einer Fusion, einem Verkauf von Vermögenswerten oder Anteilen, einer Restrukturierung, einer Finanzierung, einem Kontrollwechsel oder einer Übernahme des gesamten oder eines Teils unseres Unternehmens, an Dritte weitergegeben werden. **Rechtliche Verpflichtungen und Rechte:** Wir können auf die unter „Welche personenbezogenen Daten wir erheben“ beschriebenen Daten zugreifen, sie aufbewahren und an Strafverfolgungsbehörden, Behörden, Urheberrechtsinhaber oder andere Dritte weitergeben, wenn wir in gutem Glauben davon ausgehen, dass dies notwendig ist, um: geltendem Recht, rechtlichen Verfahren oder behördlichen Anfragen in Übereinstimmung mit international anerkannten Standards nachzukommen; die Rechte, das Eigentum und die Sicherheit unserer Nutzer, der Inhaber von Urheberrechten und anderer Personen zu schützen, einschließlich des Schutzes von Menschenleben oder der Verhinderung drohender körperlicher Schäden. So können wir beispielsweise Daten (wie Ihre IP-Adresse) an die Strafverfolgungsbehörden weitergeben, wenn in einem Notfall das Leben oder die Sicherheit einer Person gefährdet ist; mögliche Verstöße gegen unsere Nutzungsbedingungen,

Richtlinien oder andere anwendbare Bestimmungen, Richtlinien oder Standards zu untersuchen und durchzusetzen; oder irreführende Aktivitäten, Urheberrechtsverletzungen oder andere illegale Aktivitäten aufzudecken, zu untersuchen, zu verhindern oder zu bekämpfen. Weitere Informationen darüber, wie wir mit Anfragen von Strafverfolgungsbehörden und öffentlichen Stellen umgehen, finden Sie in unseren Richtlinien zur Datenanforderung bei Gesetzesvollstreckung. Unsere Rechtsgrundlagen und wie wir Ihre personenbezogenen Daten verarbeiten: Wir verwenden Ihre Daten nur, wenn wir eine „Rechtsgrundlage“ dafür haben. Je nachdem, warum wir Ihre Daten verwenden (mit anderen Worten: je nach „Zweck“ unserer Verarbeitung), nutzen wir unterschiedliche Rechtsgrundlagen. Zu diesen Rechtsgrundlagen gehören die vertragliche Erforderlichkeit, berechnete Interessen (unsere, Ihre oder die einer anderen Partei), Einwilligung, die Erfüllung einer rechtlichen Verpflichtung, die Wahrnehmung einer Aufgabe im öffentlichen Interesse und der Schutz lebenswichtiger Interessen. Hier erläutern wir die Rechtsgrundlagen, auf die wir uns bei der Verarbeitung Ihrer Daten stützen. In diesem Abschnitt wird auch beschrieben, warum wir Ihre Daten verwenden, wie diese Daten verarbeitet werden, um welche Datenkategorien es sich handelt und welche Rechte damit verbunden sind (wozu immer auch das Recht auf Auskunft zu Ihren Daten gehört). Weitere Informationen darüber, wie Sie Ihre Rechte ausüben können, finden Sie im Abschnitt „Ihre Rechte und Wahlmöglichkeiten“ in der Datenschutzerklärung. Vertragliche Erforderlichkeit: Wir verwenden die von Ihnen bereitgestellten Daten, automatisch erhobenen Daten und Daten aus anderen Quellen, wenn dies zur Erfüllung des Vertrages, den Sie bei der Registrierung, dem Zugang oder der Nutzung der Plattform eingehen (unsere Nutzungsbedingungen), erforderlich ist. Das bedeutet, dass wir Ihre Daten verwenden, um: Ihnen die Plattform zur Verfügung stellen. Wir verwenden Ihre Daten, um Ihnen den Zugriff auf die Plattform und deren Nutzung zu ermöglichen, einschließlich der Möglichkeit, Inhalte zu erstellen und zu konsumieren, mit anderen zu interagieren, soziale Funktionen zu nutzen und Ihnen Produkte und Dienstleistungen anzubieten, die Sie erwerben. Wir personalisieren auch Ihre Erfahrungen auf der Plattform, z. B. durch die Bereitstellung Ihres „Für dich“-Feeds, der Ihnen Videos zeigt, von denen wir glauben, dass sie Sie interessieren würden (weitere Informationen finden Sie hier) und durch das Vorschlagen von Konten. Unsere Nutzungsbedingungen, Richtlinien oder Bestimmungen durchzusetzen: Wir verwenden Ihre Daten, um unsere Nutzungsbedingungen, Richtlinien und Grundsätze durchzusetzen. Dies kann die Entfernung von Inhalten (auch durch automatisierte Mittel) oder die Sperrung Ihres Kontos beinhalten, wenn wir feststellen, dass Sie gegen unsere Nutzungsbedingungen oder Richtlinien verstoßen. Unsere Dienste zu verwalten: Wir verwenden die uns vorliegenden Daten auch zur Verwaltung unserer Dienste, z. B. um mit Ihnen über dienstleistungsbezogene Angelegenheiten zu kommunizieren und Ihre Anfragen zu beantworten (auch wenn Sie uns ein Problem mitteilen oder eine Kopie Ihrer Daten anfordern). Ihre Rechte: Wann immer wir Ihre Daten auf der Grundlage verwenden, dass sie für den Vertrag, den wir mit Ihnen haben, erforderlich sind, haben Sie das Recht, die von Ihnen zur Verfügung gestellten Daten zu portieren. Berechnete Interessen: Wir verwenden Ihre Daten, wenn dies zur Wahrung berechtigter Interessen erforderlich ist – unabhängig davon, ob diese uns, Sie oder einen Dritten betreffen – vorausgesetzt, dass diese Interessen nicht durch Ihre Interessen oder Grundrechte und -freiheiten überwogen werden. Wir verwenden Ihre Daten, um: Zu ermöglichen, dass Ihre Videos in interaktiven Funktionen verwendet werden können. Unsere interaktiven Funktionen wie Duett und Stitch ermöglichen es anderen Nutzern, Ihre Videos in eigene Videos einzubinden (wenn Sie dies in Ihren Einstellungen erlauben). Berechnetes Interesse, auf das wir uns berufen: Den Nutzern Tools zur Verfügung zu stellen, die zu Kreativität, Zusammenarbeit und Vergnügen anregen, und den Nutzern die Möglichkeit zu geben, neue Zielgruppen zu erreichen. Verwendete Daten: Von Ihnen bereitgestellte Daten und automatisch erhobene Daten. Ihr Konto anderen Nutzern vorzuschlagen: Wir können Ihr Konto anderen Nutzern vorschlagen, z. B. wenn ein Nutzer seine Kontakte mit der Plattform synchronisieren möchte. Berechnetes Interesse, auf das wir uns berufen: Um es den Nutzern zu ermöglichen, schnell und effizient andere Nutzer auf unserer Plattform zu finden und sich mit ihnen zu verbinden. Verwendete Daten: Von Ihnen bereitgestellte Daten, automatisch erhobene Daten und Daten aus anderen Quellen. Allen Nutzern nicht-personalisierte Werbung bereitzustellen. Wir zeigen allen Nutzern nicht-personalisierte Werbung, auch denjenigen, die sich gegen personalisierte Werbung entschieden haben. Berechnetes Interesse, auf das wir uns berufen: Wir zeigen nicht-personalisierte Werbung, um unsere Plattform kostenlos zu halten. Wir verarbeiten begrenzte Kategorien Ihrer Daten, um sicherzustellen, dass unser Werbedienst für unsere Werbekunden nützlich ist (z. B. um Nutzern in einem bestimmten Land oder Nutzern, die dieselbe Sprache sprechen, Werbung anzuzeigen). Verwendete Daten: Automatisch erhobene Daten und Daten aus anderen Quellen. Bereitstellung von Mess- und Analysediensten: Wir helfen Creator*innen und Werbetreibenden dabei, die Wirksamkeit und Verbreitung von Anzeigen und anderen Inhalten, die auf der Plattform angezeigt werden, zu messen. Berechnetes Interesse, auf das wir uns berufen: Damit Creator*innen und Werbetreibende sehen und verstehen können, wie ihre Anzeigen oder Inhalte abschneiden und welches Publikum ihre Anzeigen oder Inhalte betrachtet oder mit ihnen

interagiert. So können sie fundierte Entscheidungen treffen (z. B. darüber, welche Art von Werbekampagnen sie durchführen wollen, welche Zielgruppe sie erreichen wollen und welche Inhalte den Nutzern am besten gefallen). Dies trägt dazu bei, dass die Werbung und andere Inhalte, die wir den Nutzern zeigen, relevant und unterhaltsam bleiben und dass die Plattform für alle Nutzer kostenlos bleibt. Verwendete Daten: Von Ihnen bereitgestellte Daten, automatisch erhobene Daten und Daten aus anderen Quellen. Gewährleistung der Sicherheit und Stabilität unserer Community. Wir verwenden Ihre Daten, um die Sicherheit und das Wohlergehen unserer Community zu gewährleisten, einschließlich der Überprüfung von Nutzerinhalten (und, falls nach geltendem Recht zulässig, von Direktnachrichten und zugehörigen Metadaten) auf Verstöße gegen unsere Nutzungsbedingungen, Richtlinien und anderen Bestimmungen. Wir schließen auch auf Ihr Alter und bitten Sie unter Umständen um zusätzliche Informationen, um Ihr Alter zu bestätigen. Berechtigtes Interesse, auf das wir uns berufen: Um die Sicherheit unserer Community zu gewährleisten, die Einhaltung unserer Richtlinien zu überprüfen und den Missbrauch der Plattform aufzudecken. Verwendete Daten: Von Ihnen bereitgestellte Daten, automatisch erhobene Daten und Daten aus anderen Quellen. Gewährleistung der Sicherheit und Stabilität der Plattform. Wir verwenden Ihre Daten, um die Stabilität und Sicherheit der Plattform zu gewährleisten, einschließlich der Identifizierung und Bekämpfung von technischen oder Sicherheitsproblemen (wie z. B. technische Bugs, Spam-Accounts und die Aufdeckung von Missbrauch, Betrug und illegalen Aktivitäten). Berechtigtes Interesse, auf das wir uns berufen: Um die Stabilität und Sicherheit der Plattform zu gewährleisten und sicherzustellen, dass sie ständig verfügbar und funktionsfähig ist. Verwendete Daten: Von Ihnen bereitgestellte Daten, automatisch erhobene Daten und Daten aus anderen Quellen. Überprüfung, Verbesserung, Bewerbung und Entwicklung der Plattform. Wir verwenden die uns zur Verfügung stehenden Daten, um zu verstehen, wie die Plattform von den Nutzern verwendet wird, und um die Plattform weiterzuentwickeln und zu verbessern, einschließlich der Schulung, Entwicklung und Verbesserung unserer Technologie, wie z. B. unserer maschinellen Lernmodelle und Algorithmen. Wir verwenden diese Informationen auch, um die Plattform, beliebte Themen und neue Trends besser zu verstehen und zu fördern. Berechtigtes Interesse, auf das wir uns berufen: Verbesserung, Bewerbung und Entwicklung der Plattform auf fundierte Art und Weise. Verwendete Daten: Von Ihnen bereitgestellte Daten, automatisch erhobene Daten und Daten aus anderen Quellen. Weitergabe Ihrer Daten an Dritte: **Wir geben Ihre Daten an Dritte weiter, deren Plattformen oder Dienste in die Plattform integriert sind.** Berechtigtes Interesse, auf das wir uns berufen: Um Ihnen ein nahtloses Erlebnis zu bieten, die Weitergabe Ihrer Inhalte auf anderen Plattformen zu ermöglichen, Dritten die Authentifizierung von Nutzern zu ermöglichen und das Nutzererlebnis zu optimieren. Verwendete Daten: Von Ihnen bereitgestellte Daten, automatisch erhobene Daten und Daten aus anderen Quellen. Kommunikation zu Marketingzwecken: Wir können Ihnen direkte Marketingnachrichten über Funktionen unserer Dienste und Dienste von Drittanbietern senden, von denen wir glauben, dass sie Sie interessieren. Wir können Ihnen auch Werbeaktionen, Wettbewerbe, Marketingkampagnen oder Veranstaltungen zusenden. Wir holen Ihre Einwilligung ein, um Ihnen Nachrichten zu senden, sofern dies gesetzlich vorgeschrieben ist. Berechtigtes Interesse, auf das wir uns berufen: Um die Plattform oder Produkte und Dienstleistungen von Dritten zu bewerben. Verwendete Daten: Von Ihnen bereitgestellte Daten, automatisch erhobene Daten und Daten aus anderen Quellen. Ihre Rechte: Wann immer wir Ihre Daten auf Grund berechtigter Interessen verwenden, können Sie dem widersprechen und die Einschränkung der Verwendung verlangen. Ihre Einwilligung: Wir holen Ihre Einwilligung ein, um auf Ihre Daten zuzugreifen oder sie für bestimmte Zwecke zu verwenden. Wenn wir dies tun, können Sie Ihre Einwilligung jederzeit über die Geräteberechtigungen oder In-App-Einstellungen widerrufen. Personalisierte Werbung: Mit Ihrer Einwilligung zeigen wir Ihnen personalisierte Werbung, die auf Ihren Aktivitäten auf der Plattform und außerhalb der Plattform basiert. Verwendete Daten: Von Ihnen zu diesem Zweck bereitgestellte Daten, automatisch erhobene Daten und Daten aus anderen Quellen. Ihre Rechte: Wann immer wir Ihre Daten auf der Grundlage Ihrer Einwilligung verwenden, können Sie Ihre Einwilligung jederzeit widerrufen. Der Widerruf Ihrer Einwilligung berührt jedoch nicht die Rechtmäßigkeit der Verarbeitung Ihrer Daten auf der Grundlage Ihrer Einwilligung vor dem Widerruf der Einwilligung. Sie können Ihre Einwilligung zu den entsprechenden Einstellungen für personalisierte Werbung widerrufen, indem Sie diese Anweisungen befolgen. Sie haben auch das Recht, Informationen, die Sie uns zur Verfügung gestellt haben und die wir auf der Grundlage Ihrer Einwilligung verwenden, zu portieren. Erfüllung einer rechtlichen Verpflichtung: Wir können Ihre Informationen, einschließlich Ihrer Profilinformationen oder Nutzerinhalte, verwenden, wenn dies erforderlich ist, um einer rechtlichen Verpflichtung nachzukommen. Dies umfasst Situationen, in denen wir verpflichtet sind, Maßnahmen zu ergreifen, um die Sicherheit unserer Nutzer zu gewährleisten oder einer rechtmäßigen Anfrage nachzukommen, wie z. B. einer Anordnung von Strafverfolgungsbehörden oder Gerichten. Wir verwenden grundsätzlich von Ihnen bereitgestellte Daten und automatisch erhobene Daten, wobei dies von der jeweiligen Situation abhängt. Erfüllung einer Aufgabe im öffentlichen Interesse: Wir können Ihre Daten verwenden, wenn dies zur Erfüllung

einer Aufgabe im öffentlichen Interesse erforderlich ist, einschließlich der Durchführung von Forschungsarbeiten, der Verhütung und Aufdeckung von Straftaten, des Schutzes von Kindern und der Förderung der öffentlichen Sicherheit und Integrität gemäß den geltenden Gesetzen. Wir verwenden grundsätzlich von Ihnen bereitgestellte Daten und automatisch erhobene Daten, wobei dies von der jeweiligen Situation abhängt. Ihre Rechte: Wenn wir Ihre Daten auf der Grundlage verwenden, dass dies für eine Aufgabe im öffentlichen Interesse erforderlich ist, haben Sie das Recht, unserer Verwendung zu widersprechen und eine diesbezügliche Einschränkung zu verlangen. Schutz lebenswichtiger Interessen von Personen: Wir können Ihre Daten verwenden, wenn dies notwendig ist, um das Leben, die körperliche Unversehrtheit oder die Sicherheit von Ihnen oder einer anderen Person zu schützen. Dies könnte die Übermittlung von Daten an Strafverfolgungsbehörden oder Notdienste in dringenden Situationen zum Schutz von Gesundheit oder Leben beinhalten. Wir stellen grundsätzlich von Ihnen bereitgestellte Daten und automatisch erhobene Daten bereit, wobei dies von der jeweiligen Situation abhängt. Ihre Rechte und Wahlmöglichkeiten: Sie haben Rechte und Wahlmöglichkeiten, wenn es um Ihre Daten geht. Einige dieser Rechte gelten allgemein, während andere nur unter bestimmten Umständen gelten. Je nach Situation können diese Rechte Einschränkungen unterliegen. TikTok Irland ist für die Beantwortung Ihrer Anfrage innerhalb der gesetzlich vorgeschriebenen Fristen verantwortlich. Falls erforderlich, wird sich TikTok Irland mit TikTok UK in Verbindung setzen, um Ihre Anfrage zu bearbeiten. Auskunft über Ihren Daten. Sie können kostenlos von uns verlangen, Ihnen zu bestätigen, welche Daten wir über Sie verarbeiten, Ihnen bestimmte Daten über die Verarbeitung zu geben und eine Kopie Ihrer Daten zu erhalten. Mit den In-App-Kontrollen können Sie: auf Ihre Daten zugreifen, die anderen Nutzern zur Verfügung stehen, indem Sie auf die Registerkarte „Profil“ in Ihrem Konto navigieren. eine Kopie Ihrer Daten anfordern, indem Sie das Tool „Deine Daten herunterladen“ nutzen. Klicken Sie hier für detaillierte Anweisungen. Löschen Ihrer Daten: Sie können Ihre Daten löschen oder uns bitten, sie ganz oder teilweise zu löschen. Mit den In-App-Kontrollen können Sie: die in Ihrem Profil veröffentlichten Inhalte löschen, wie z. B. Ihre Nutzerinhalte und Ihre Profilinformationen. Ihr gesamtes Konto löschen. Klicken Sie hier für detaillierte Anweisungen: die Löschung eines bestimmten Inhalts mithilfe der In-App-Meldefunktion beantragen. (Weitere Informationen finden Sie hier). Berichtigung Ihrer Daten: Sie können Ihre Daten ändern oder uns auffordern, sie zu ändern oder zu korrigieren, wenn diese Daten nicht korrekt sind. Sie können viele Ihrer Daten über die In-App-Kontrollen und Einstellungen ändern oder korrigieren (z. B. Ihre Profilinformationen und Videoinhalte). Übertragbarkeit Ihrer Daten: Sie haben das Recht auf Datenübertragbarkeit in Fällen, in denen wir uns auf die vertragliche Erforderlichkeit und die Einwilligung als Rechtsgrundlage stützen. Das bedeutet, dass Sie das Recht haben, Ihre Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und sie an einen Dritten weiterzugeben. Sie können von Ihrem Recht auf Datenübertragbarkeit Gebrauch machen, indem Sie in Ihren Einstellungen die Option „Deine Daten herunterladen“ wählen. Klicken Sie hier für detaillierte Anweisungen. Widerspruch gegen die Verarbeitung Ihrer Daten. Sie haben auch das Recht, Widerspruch gegen die Verarbeitung Ihrer Daten einzulegen. Dieses Recht gilt, wenn wir eine Aufgabe im öffentlichen Interesse wahrnehmen oder unsere berechtigten Interessen oder die eines Dritten verfolgen. Wenn Sie einen Widerspruch einlegen, geben Sie bitte alle relevanten Informationen an, einschließlich der Verarbeitung, gegen die Sie Widerspruch einlegen, warum Sie Widerspruch einlegen möchten und wie die Verarbeitung Sie betrifft, sowie alle zusätzlichen Informationen, die uns Ihrer Meinung nach bei der Prüfung Ihres Antrags helfen. Wir werden die betreffende Verarbeitung einstellen, wenn wir keine zwingenden legitimen Gründe haben, diese Verarbeitung fortzusetzen, oder wenn wir sie nicht für rechtliche Ansprüche benötigen. Einschränkung der Verarbeitung Ihrer Daten: Sie haben das Recht, die Einschränkung der Verarbeitung Ihrer Daten zu verlangen, wenn (a) Sie die Richtigkeit der Daten beanstanden, (b) die Daten unrechtmäßig verarbeitet wurden, Sie aber gegen die Löschung dieser Daten widersprechen, (c) die Daten für die Verfolgung oder Verteidigung eines Rechtsanspruchs aufbewahrt werden müssen, oder (d) Sie der Verarbeitung widersprochen haben und das Ergebnis dieses Widerspruchs abwarten. Um die oben genannten Rechte auszuüben, kontaktieren Sie uns bitte über unser Webformular. Bevor wir auf eine Anfrage zur Ausübung eines oder mehrerer der oben genannten Rechte reagieren können, müssen Sie möglicherweise Ihre Identität oder Ihre Kontoinformationen bestätigen oder zusätzliche Informationen zur Verfügung stellen, damit wir den Vorgang verstehen können. Wir ermutigen Sie, uns zu „kontaktieren“, wenn Sie mit der Art und Weise, wie wir auf eine Ihrer Anfragen zu Ihren Rechten reagiert haben, nicht zufrieden sind. Sie haben auch das Recht, eine Beschwerde bei der irischen Datenschutzkommission (der federführenden Aufsichtsbehörde von TikTok Irland) oder bei Ihrer örtlichen Aufsichtsbehörde einzureichen. Zusätzlich zu diesen Rechten können Sie die Datenschutzeinstellungen für Ihr Konto kontrollieren. Klicken Sie hier für weitere Informationen. Datensicherheit und -aufbewahrung: Die Sicherheit Ihrer Daten ist uns wichtig. Wir ergreifen angemessene technische, administrative und physische Sicherheitsmaßnahmen, um Ihre Daten vor unbefugtem Zugriff, Diebstahl, Offenlegung, Änderung oder Verlust zu schützen. Wir überprüfen

unsere Sicherheitsmaßnahmen regelmäßig, um verfügbare neue Technologien und Methoden zu berücksichtigen. Wir bewahren Ihre Daten so lange auf, wie es für die Bereitstellung der Plattform und für die anderen in dieser Datenschutzerklärung genannten Zwecke erforderlich ist. Wir bewahren die Daten auch auf, wenn dies zur Erfüllung vertraglicher und rechtlicher Verpflichtungen erforderlich ist, wenn wir ein berechtigtes Geschäftsinteresse daran haben (z. B. zur Verbesserung und Entwicklung der Plattform und zur Verbesserung der Sicherheit und Stabilität unserer Dienste) und zur Geltendmachung oder Verteidigung von Rechtsansprüchen. Die Aufbewahrungsfristen sind je nach Art der Daten und den Zwecken, für die wir die Daten verwenden, unterschiedlich. Wenn wir zum Beispiel Ihre Daten verarbeiten, um Ihnen die Plattform zur Verfügung zu stellen, bewahren wir diese Daten so lange auf, wie Sie ein TikTok-Konto haben. **Zu diesen Daten gehören Ihre Profilinformatio- nen, Nutzerinhalte und Direktnachrichten.** Wenn Sie gegen unsere Richtlinien oder Nutzungsbedingungen verstoßen, können wir Ihre Profilinformatio- nen und/oder Nutzerinhalte sofort aus der öffentlichen Ansicht entfernen, aber Ihre Daten so lange aufbewahren, wie es für die Bearbeitung des Verstoßes erforderlich ist. Unsere globalen Aktivitäten und Datenübertragungen: **Wir speichern die unter „Welche personenbezogenen Daten wir erheben“ beschriebenen Daten auf sicheren Servern in den Vereinigten Staaten und in Singapur.** Bestimmte Unternehmen unserer Unternehmensgruppe, die sich außerhalb Ihres Wohnsitzlandes befinden (siehe hier), erhalten, wie im Abschnitt „Unsere Unternehmensgruppe“ unter „Wie wir Ihre personenbezogenen Daten weitergeben“ beschrieben, **einen begrenzten Fernzugriff auf diese Daten**, damit sie bestimmte wichtige Funktionen bereitstellen können. Dieser Zugriff ist begrenzt und sicher. Er wird nur soweit notwendig und unter strengen Sicherheitskontrollen und Verfahren zur Genehmigung von Berechtigungen gewährt. Wir geben die unter „Welche personenbezogenen Daten wir erheben“ beschriebenen Daten, wie unter „Wie wir Ihre personenbezogenen Daten weitergeben“ beschrieben, an Dienstanbieter, Partner und sonstige Drittunternehmen weiter. Diese Dritten können sich außerhalb Ihres Wohnsitzlandes befinden. Diese Unternehmen verpflichten sich, Ihre Daten in Übereinstimmung mit den geltenden Datenschutzgesetzen zu verarbeiten und angemessene Sicherheitsmaßnahmen zum Schutz Ihrer Daten zu ergreifen. Wenn wir Ihre Daten außerhalb des Europäischen Wirtschaftsraums (EWR), des Vereinigten Königreichs oder der Schweiz übermitteln, stellen wir sicher, dass ihnen ein angemessenes Datenschutzniveau zu Gute kommt, indem wir: Uns auf Angemessenheitsbeschlüsse stützen. Dabei handelt es sich um Entscheidungen der Europäischen Kommission gemäß Artikel 45 DSGVO (oder gleichwertige Entscheidungen anderer zuständiger Behörden), in denen festgestellt wird, dass ein Land (außerhalb des EWR) ein angemessenes Datenschutzniveau bietet. Wir übermitteln Ihre Daten, wie unter „Welche personenbezogenen Daten wir erheben“ beschrieben, an Länder mit Angemessenheitsbeschlüssen, wie z. B. die hier aufgeführten Länder; oder Standardvertragsklauseln. Die Europäische Kommission hat Vertragsklauseln gemäß Artikel 46 der Datenschutz-Grundverordnung genehmigt, die es Unternehmen im EWR ermöglichen, Daten in Länder außerhalb des EWR zu übertragen. Diese (sowie die gleichwertigen für das Vereinigte Königreich und die Schweiz genehmigten Vertragsklauseln) werden als **Standardvertragsklauseln** bezeichnet. Wir stützen uns auf Standardvertragsklauseln, um Daten, wie unter „Welche personenbezogenen Daten wir erheben“ beschrieben, an bestimmte Unternehmen unserer Unternehmensgruppe (wie hier dargelegt) und an Dritte in Ländern ohne Angemessenheitsbeschluss zu übermitteln. Ein Exemplar dieser Standardvertragsklauseln oder Angemessenheitsbeschlüsse erhalten Sie, wenn Sie sich über die im Abschnitt „Kontaktieren Sie uns“ unten angegebenen Kontaktdaten mit uns in Verbindung setzen. Minderjährige Nutzer: Sie müssen mindestens 13 Jahre alt sein, um die Plattform nutzen zu dürfen. Wenn Sie der Meinung sind, dass wir Daten über eine Person haben, die jünger ist als 13 Jahre, kontaktieren Sie uns bitte über die im Abschnitt „Kontaktieren Sie uns“ unten angegebenen Kontaktdaten. Um Nutzern unter 18 Jahren ein altersgerechtes Erlebnis zu bieten, sind bestimmte Funktionen nicht verfügbar. Weitere Einzelheiten finden Sie in unserem Hilfe-Center. Wenn Sie der Vormund eines Teenagers sind, finden Sie in unserem Leitfaden für Erziehungsberechtigte Informationen und Ressourcen, die Ihnen helfen, die Plattform und die Tools und Kontrollen zu verstehen, die Sie oder Ihr Teenager nutzen können, einschließlich der „Begleiteter Modus“-Funktionen. Aktualisierungen der Datenschutzerklärung: Wir können diese Datenschutzerklärung von Zeit zu Zeit ändern oder aktualisieren. Wir werden Sie über alle wesentlichen Änderungen dieser Datenschutzerklärung durch eine Mitteilung auf der Plattform oder auf anderem Wege informieren. Das Datum „Letzte Aktualisierung“ oben in dieser Datenschutzerklärung spiegelt das Datum des Inkrafttretens solcher Änderungen wider. Kontaktieren Sie uns: Sie können uns bezüglich dieser Datenschutzerklärung über unser Webformular kontaktieren. Sie können den Datenschutzbeauftragten von TikTok hier erreichen. Sie können uns auch unter der folgenden Postanschrift erreichen. Für Nutzer aus dem Europäischen Wirtschaftsraum und der Schweiz: TikTok Technology Limited, 10 Earlsfort Terrace, Dublin, D02 T380, Irland. Für Nutzer aus dem Vereinigten Königreich: TikTok Information Technologies UK Limited, 4 Lindsey Street, Barbican, London, EC1A 9HP, United Kingdom, Vereinigtes Königreich.

Instagram-Datenschutzrichtlinie

Diese Richtlinie beschreibt die Informationen, die wir zur Unterstützung von Facebook, Instagram, Messenger und anderen von Facebook angebotenen Produkten und Funktionen (Facebook-Produkte oder Produkte) verarbeiten. Zusätzliche Tools und Informationen findest du in den Facebook-Einstellungen und den Instagram-Einstellungen.

I. Welche Arten von Informationen erfassen wir?

Zur Bereitstellung der Facebook-Produkte müssen wir Informationen über dich verarbeiten. Die Arten der von uns erfassten Informationen hängen davon ab, wie du unsere Produkte nutzt. Du kannst erfahren, wie du auf von uns erfasste Informationen zugreifen bzw. sie löschen kannst, indem du die Facebook-Einstellungen bzw. die Instagram-Einstellungen besuchst.

Von dir und anderen getätigte und bereitgestellte Dinge.

Von dir bereitgestellte Informationen und Inhalte. Wir erfassen die Inhalte, Kommunikationen und sonstigen Informationen, die du bereitstellst, wenn du unsere Produkte nutzt; dazu gehören auch deine Registrierung für ein Konto, das Erstellen oder Teilen von Inhalten sowie der Nachrichtenaustausch bzw. das Kommunizieren mit anderen. Dies kann Informationen über die von dir bereitgestellten Inhalte oder solche, die in ihnen enthalten sind (wie Metadaten) umfassen, wie z. B. den Aufnahme-Standort eines Fotos oder das Datum, an dem eine Datei erstellt wurde. Es kann auch das umfassen, was du durch von uns bereitgestellte Funktionen, wie z. B. unsere Kamera, siehst, damit wir dir beispielsweise Masken und Filter, die dir gefallen könnten, vorschlagen oder dir Tipps für die Verwendung des Hochformats geben können. Unsere Systeme verarbeiten von dir bereitgestellte Inhalte und Mitteilungen automatisch, um den Kontext und die in ihnen enthaltenen Details für die unten beschriebenen Zwecke zu analysieren. Erfahre mehr darüber, wie du kontrollieren kannst, wer die Dinge sehen kann, die du teilst.

Daten mit besonderem Schutz: Du kannst in deinen Facebook-Profilfeldern oder unter „Lebensereignisse“ Informationen über deine religiösen Ansichten, deine politischen Einstellungen oder deine Gesundheit bzw. an wem du „interessiert“ bist angeben. Diese und andere Informationen (wie etwa Nationalität oder ethnische Herkunft, weltanschauliche Überzeugungen oder eine Gewerkschaftszugehörigkeit) unterliegen nach EU-Recht einem besonderen Schutz.

Netzwerke und Verbindungen. Wir erfassen Informationen über die Personen, Seiten, Konten, Hashtags und Gruppen, mit denen du verbunden bist, und darüber, wie du mit ihnen in unseren Produkten interagierst; dies sind beispielsweise Personen, mit denen du am meisten kommunizierst, oder Gruppen, denen du angehörst. Außerdem sammeln wir Kontaktinformationen, wenn du diese von einem Gerät hochlädst, synchronisierst oder importierst (wie z. B. ein Adressbuch oder Anrufprotokoll oder eine SMS-Protokollhistorie).

Diese verwenden wir beispielsweise, um dir und anderen dabei zu helfen, Personen zu finden, die du möglicherweise kennst, sowie für die anderen unten aufgeführten Zwecke.

Deine Nutzung. Wir erfassen Informationen darüber, wie du unsere Produkte nutzt, beispielsweise über die Arten von Inhalten, die du dir ansiehst bzw. mit denen du interagierst, über die von dir genutzten Funktionen, über die von dir durchgeführten Handlungen, über die Personen oder Konten, mit denen du interagierst, und über die Zeit, Häufigkeit und Dauer deiner Aktivitäten. Zum Beispiel protokollieren wir, wenn du unsere Produkte gerade nutzt bzw. wann du diese zuletzt genutzt hast, und welche Beiträge, Videos und sonstigen Inhalte du dir in unseren Produkten ansiehst. Wir erfassen auch Informationen darüber, wie du Funktionen wie unsere Kamera nutzt.

Informationen über auf unseren Produkten durchgeführte Transaktionen. Wenn du unsere Produkte für Käufe oder andere finanzielle Transaktionen nutzt (beispielsweise wenn du einen Kauf in einem Spiel tätigst oder etwas spendest), erfassen wir Informationen über den Kauf bzw. die Transaktion. Dies beinhaltet Zahlungsinformationen, wie deine Kredit- oder Debitkartennummer und andere Karteninformationen, sonstige Konto- und Authentifizierungsinformationen sowie Abrechnungs-, Versand- und Kontaktangaben. Aktivitäten anderer und von ihnen über dich bereitgestellte Informationen. Außerdem erhalten und analysieren wir Inhalte, Kommunikationen und Informationen, die andere Personen bereitstellen, wenn sie unsere Produkte nutzen. Dies können auch Informationen über dich sein, beispielsweise, wenn andere ein Foto von dir teilen oder kommentieren, dir eine Nachricht senden bzw. deine Kontaktinformationen hochladen, synchronisieren oder importieren.

Geräteinformationen

Wie unten beschrieben, erfassen wir Informationen von und über von dir genutzte(n) Computer(n), Telefone(n), Connected TVs und andere(n) mit dem Internet verbundene(n) Geräte(n), die über eine Integration mit unseren Produkten verfügen. Diese Informationen kombinieren wir dann über verschiedene von dir genutzte Geräte hinweg. Zum Beispiel verwenden wir Informationen, die wir über deine Nutzung unserer Produkte auf deinem Telefon gesammelt haben, für eine bessere Personalisierung der Inhalte (einschließlich Werbeanzeigen) oder Funktionen, die du siehst, wenn du unsere Produkte auf einem anderen Gerät nutzt, wie z. B. deinem Laptop oder Tablet, oder um zu messen, ob du als Reaktion auf eine Werbeanzeige, die wir dir auf deinem Telefon gezeigt haben, auf einem anderen Gerät eine Handlung vorgenommen hast.

Die Informationen, die wir von diesen Geräten erhalten, beinhalten:

Geräteattribute: Informationen wie das Betriebssystem, Hardware- und Software-Versionen, Batteriestand, Signalstärke, verfügbarer Speicherplatz, Browsertyp, App- und Dateinamen und -arten sowie Plugins.

Vorgänge auf dem Gerät: Informationen über die auf dem Gerät durchgeführten Vorgänge und Tätigkeiten, beispielsweise ob sich ein Fenster im Vordergrund oder Hintergrund befindet oder Mausbewegungen (das kann dabei helfen, Menschen von Robotern zu unterscheiden).

Identifikatoren: **Eindeutige Identifikatoren, Geräte-IDs und sonstige Identifikatoren**, wie solche von Spielen, Apps oder Konten, die du nutzt, und **Familiengeräte-IDs** (oder sonstige Identifikatoren, die für die mit demselben Gerät oder Konto verknüpften Produkte der Facebook-Unternehmen eindeutig sind).

Gerätesignale: Bluetooth-Signale und Informationen über WLAN-Zugangspunkte, Beacons und Funkzelltürme in der Nähe.

Daten aus den Geräteeinstellungen: Informationen, deren Erhalt du uns durch die von dir aktivierten Geräteeinstellungen gestattest, wie den **Zugriff auf deinen GPS-Standort, deine Kamera oder Fotos.**

Netzwerk und Verbindungen: Informationen wie der **Name deines Mobilfunk- oder Internetanbieters, die Sprache, Zeitzone, Mobiltelefonnummer, IP-Adresse oder Verbindungsgeschwindigkeit** und in einigen Fällen Informationen über andere in der Nähe oder in deinem Netzwerk befindliche Geräte, damit wir dich dabei unterstützen können, beispielsweise ein Video von deinem Telefon auf deinen Fernseher zu streamen.

Cookie-Daten: Daten von auf deinem Gerät gespeicherten Cookies, einschließlich **Cookie-IDs und -Einstellungen**. Erfahre in der Facebook-Cookie-Richtlinie und der Instagram-Cookie-Richtlinie mehr darüber, wie wir Cookies verwenden.

Informationen von Partnern.

Werbetreibende, App-Entwickler und -Publisher können uns über die von ihnen genutzten Facebook Business-Tools, u. a. unsere sozialen Plugins (wie den „Gefällt mir“-Button), Facebook Login, unsere APIs und SDKs oder das Facebook-Pixel, Informationen senden. Diese Partner stellen uns Informationen über deine Aktivitäten außerhalb von Facebook bereit, u. a. Informationen über dein Gerät, von dir besuchte Websites, von dir getätigte Käufe, Werbeanzeigen, die du siehst und darüber, wie du ihre Dienste nutzt, und zwar unabhängig davon, ob du ein Facebook-Konto hast oder bei Facebook eingeloggt bist. Beispielsweise könnte ein Spieleentwickler unsere API nutzen, um uns mitzuteilen, welche Spiele du spielst, oder ein Unternehmen könnte uns von einem Kauf berichten, den du in seinem Geschäft getätigt hast. Wir erhalten außerdem Informationen über deine Online- und Offline-Handlungen und -Käufe von Dritt-Datenanbietern, die berechtigt sind, uns deine Informationen bereitzustellen.

Partner erhalten deine Daten, wenn du ihre Dienste besuchst oder nutzt, oder durch Dritte, mit denen sie zusammenarbeiten. Wir verlangen von jedem dieser Partner, dass er die gesetzlich festgelegten Rechte besitzt, deine Daten zu erfassen, zu verwenden und zu teilen, bevor er uns irgendwelche Daten bereitstellt. Erfahre mehr über die Arten von Partnern, von denen wir Daten erhalten.

Lies dir die Facebook-Cookie-Richtlinie und die Instagram-Cookie-Richtlinie durch, um mehr darüber zu erfahren, wie wir Cookies in Verbindung mit Facebook Business Tools verwenden.

II. Wie verwenden wir diese Informationen?

Wir verwenden die uns zur Verfügung stehenden Informationen (vorbehaltlich der von dir getroffenen Auswahl) so, wie es weiter unten beschrieben ist, und um die Facebook-Produkte und zugehörigen Dienste, wie in den Facebook-Nutzungsbedingungen und den Instagram-Nutzungsbedingungen beschrieben, bereitzustellen und zu unterstützen. Dies geschieht folgendermaßen:

Bereitstellung, Personalisierung und Verbesserung unserer Produkte.

Wir verwenden die uns zur Verfügung stehenden Informationen, um unsere Produkte bereitzustellen, also auch um Funktionen und Inhalte (u. a. deinen News Feed, deinen Instagram Feed, deine Instagram Stories und deine Werbeanzeigen) zu personalisieren und dir auf und außerhalb von unseren Produkten Vorschläge zu unterbreiten (wie z. B. Gruppen oder Veranstaltungen, an denen du möglicherweise interessiert bist, oder Themen, die du eventuell abonnieren möchtest). Um personalisierte Produkte zu erstellen, die individuell und für dich relevant sind, verwenden wir deine Verbindungen, Präferenzen, Interessen und Aktivitäten. Dies basiert auf den Daten, die wir von dir und anderen erfassen und erfahren (einschließlich jedweder von dir bereitgestellten Daten mit besonderem Schutz, für die du uns deine ausdrückliche Einwilligung gegeben hast); darauf, wie du unsere Produkte nutzt und mit ihnen interagierst, und auf den Personen, Orten oder Dingen, mit denen du auf und außerhalb von unseren Produkten verbunden bzw. an denen du interessiert bist. Erfahre mehr darüber, wie wir Informationen über dich verwenden, um dein Facebook- und Instagram-Erlebnis, einschließlich Funktionen, Inhalten und Empfehlungen auf Facebook-Produkten, zu

personalisieren. Du kannst auch mehr dazu erfahren, wie wir die Werbeanzeigen auswählen, die du siehst.

Informationen über verschiedene Facebook-Produkte und Geräte hinweg: Wir verbinden Informationen über deine Aktivitäten auf verschiedenen Facebook-Produkten und Geräten miteinander, um dir ein individuelleres und einheitlicheres Erlebnis in allen von dir genutzten Facebook-Produkten bereitzustellen, gleichgültig, wo du sie nutzt. Wir können dir beispielsweise vorschlagen, einer Gruppe auf Facebook beizutreten, der Personen angehören, denen du auf Instagram folgst oder mit denen du im Messenger kommunizierst. Außerdem können wir dein Erlebnis nahtloser gestalten, indem wir beispielsweise automatisch deine Registrierungsinformationen (wie deine Telefonnummer) von einem Facebook-Produkt eingeben, wenn du dich auf einem anderen Produkt für ein Konto registrierst.

Standortbezogene Informationen: Wir verwenden standortbezogene Informationen – wie deinen aktuellen Standort, deinen Wohnort, die Orte, die du gerne besuchst, und die Unternehmen und Personen in deiner Nähe – um dir und anderen unsere Produkte, einschließlich Werbeanzeigen, bereitzustellen und diese zu verbessern. Standortbezogene Informationen können auf Dingen wie dem genauen Gerätestandort (wenn du uns gestattet hast, diesen zu erheben), IP-Adressen sowie Informationen aus der Nutzung von Facebook-Produkten durch dich und andere (wie besuchte Orte oder Veranstaltungen, an denen du teilgenommen hast) basieren.

Produktforschung und -entwicklung: Wir verwenden die uns zur Verfügung stehenden Informationen zur Entwicklung, Erprobung und Verbesserung unserer Produkte, u. a. indem wir Umfragen und Studien sowie Tests und Fehler- bzw. Problembhebungen für neue Produkte und Funktionen durchführen.

Gesichtserkennung: Wenn du dies aktiviert hast, nutzen wir Gesichtserkennungstechnologie, um dich auf Fotos bzw. in Videos und Kameraerlebnissen wiederzuerkennen. Bei den von uns erstellten Gesichtserkennungsvorlagen handelt es sich gemäß EU-Recht um Daten mit besonderem Schutz. Erfahre mehr darüber, wie wir Gesichtserkennungstechnologie einsetzen. Du kannst unsere Nutzung dieser Technologie in den Facebook-Einstellungen kontrollieren. Falls wir Gesichtserkennungstechnologie für dein Instagram-Erlebnis einführen, werden wir dich darüber vorab informieren. Du kannst dann kontrollieren, ob wir diese Technologie für dich einsetzen.

Werbeanzeigen und andere gesponserte Inhalte: Wir verwenden die uns über dich zur Verfügung stehenden Informationen – einschließlich Informationen über deine Interessen, Handlungen und Verbindungen – um die Werbeanzeigen, Angebote und sonstigen gesponserten Inhalte auszuwählen und zu personalisieren, die wir dir zeigen. Mehr dazu, wie wir Werbeanzeigen auswählen und personalisieren, und welche Auswahlmöglichkeiten du bezüglich der von uns für die Auswahl der Werbeanzeigen und sonstigen gesponserten Inhalte verwendeten Daten hast, erfährst du in den Facebook-Einstellungen und Instagram-Einstellungen.

Bereitstellung von Messungen, Analysen und sonstigen Unternehmens-Services.

Wir verwenden die uns zur Verfügung stehenden Informationen (einschließlich deiner Aktivitäten außerhalb unserer Produkte, wie z. B. die von dir besuchten Webseiten und die Werbeanzeigen, die du siehst), um Werbetreibenden und anderen Partnern zu helfen, die Effektivität und Verbreitung ihrer Werbeanzeigen und Dienste zu messen und Aufschluss über die Arten von Personen, die ihre Dienste nutzen, sowie darüber, wie Personen mit

ihren Webseiten, Apps und Diensten interagieren, zu erlangen. So teilen wir Informationen mit diesen Partnern.

Förderung von Schutz, Integrität und Sicherheit.

Wir verwenden die uns zur Verfügung stehenden Informationen, um auf und außerhalb von unseren Produkten Aktivitäten und Konten zu verifizieren, schädliches Verhalten zu bekämpfen, Spam und andere negative Erlebnisse aufzudecken und zu verhindern, die Integrität unserer Produkte zu wahren und den Schutz sowie die Sicherheit zu fördern. Zum Beispiel verwenden wir uns zur Verfügung stehende Daten, um verdächtige Aktivitäten oder Verstöße gegen unsere Nutzungsbedingungen oder Richtlinien zu untersuchen oder um festzustellen, wenn jemand Hilfe benötigt. Mehr dazu erfährst du im Facebook-Hilfebereich unter „Sicherheit“ und in den Instagram-Sicherheitstipps.

Kommunikation mit dir.

Wir verwenden die uns zur Verfügung stehenden Informationen, um dir Marketingkommunikationen zu senden, um mit dir über unsere Produkte zu kommunizieren und um dich über unsere Richtlinien und Nutzungsbedingungen zu informieren. Deine Informationen verwenden wir auch, um dir zu antworten, wenn du uns kontaktierst.

Forschung und Innovation für soziale Zwecke.

Wir verwenden die uns zur Verfügung stehenden Informationen (u. a. von Forschungspartnern, mit denen wir zusammenarbeiten), um Forschung und Innovation zu Themen des sozialen Allgemeinwohls, des technologischen Fortschritts, des öffentlichen Interesses, der Gesundheit und des Wohlergehens durchzuführen und zu unterstützen. Beispielsweise analysieren wir die uns über Migrationsmuster in Krisensituationen zur Verfügung stehenden Informationen, um Hilfsmaßnahmen zu unterstützen. Mehr zu unseren Forschungsprogrammen.

III. Wie werden diese Informationen geteilt?

Deine Informationen werden folgendermaßen mit anderen geteilt:

Teilen auf Facebook-Produkten

Personen und Konten, mit denen du Inhalte teilst bzw. kommunizierst

Wenn du unter Nutzung unserer Produkte Inhalte teilst und kommunizierst, wählst du die Zielgruppe für die Inhalte aus, die du teilst. Wenn du beispielsweise etwas auf Facebook postest, wählst du die Zielgruppe für den Beitrag aus: z. B. eine Gruppe, alle deine Freunde/Freundinnen, öffentlich oder eine benutzerdefinierte Personenliste. Ebenso gilt: Wenn du Messenger oder Instagram nutzt, um mit Personen oder Unternehmen zu kommunizieren, können diese Personen und Unternehmen die Inhalte sehen, die du sendest. Außerdem kann dein Netzwerk die Handlungen sehen, die du auf unseren Produkten durchgeführt hast, einschließlich Interaktionen mit Werbeanzeigen und gesponserten Inhalten. Wir zeigen anderen Konten auch, wer ihre Facebook oder Instagram Stories angesehen hat.

Öffentliche Informationen können von jedem auf oder außerhalb von unseren Produkten gesehen werden, also auch, wenn er/sie kein Konto hat. Dies umfasst auch deinen Instagram-Benutzernamen, jedwede Informationen, die du mit einer öffentlichen Zielgruppe teilst, sowie Informationen in deinem öffentlichen Profil auf Facebook bzw. Inhalte, die du auf einer Facebook-Seite, einem öffentlichen Instagram-Konto oder in irgendeinem sonstigen öffentlichen Forum wie z. B. Facebook Marketplace teilst. Du, andere Personen,

die Facebook und Instagram nutzen, und wir können jedem auf oder außerhalb von unseren Produkten Zugriff auf öffentliche Informationen gewähren oder ihm/ihr öffentliche Informationen senden, also auch auf anderen Produkten der Facebook-Unternehmen, in Suchergebnissen oder über Tools und APIs. Auf öffentliche Informationen kann auch über Drittanbieter-Dienste, wie Suchmaschinen, APIs und Offline-Medien (z. B. Fernsehen) und von Apps, Webseiten und anderen Diensten, die über eine Integration mit unseren Produkten verfügen, zugegriffen werden bzw. sie können über diese gesehen, erneut geteilt oder heruntergeladen werden.

Erfahre mehr darüber, welche Informationen öffentlich sind und wie du deine Sichtbarkeit auf Facebook und Instagram kontrollieren kannst.

Inhalte, die andere über dich (erneut) teilen

Du solltest dir gut überlegen, mit wem du Inhalte teilst, da die Personen, die deine Aktivität auf unseren Produkten sehen können, die Inhalte mit anderen auf und außerhalb von unseren Produkten teilen können, einschließlich Personen und Unternehmen, die nicht zu der Zielgruppe gehören, mit der du die Inhalte geteilt hast. Wenn du zum Beispiel einen Beitrag teilst oder eine Nachricht an bestimmte Freunde/Freundinnen oder Konten sendest, können sie diesen Inhalt herunterladen, einen Screenshot davon anfertigen oder ihn erneut mit anderen auf oder außerhalb von unseren Produkten, in persönlichen Erlebnissen oder solchen der virtuellen Realität wie Facebook Spaces teilen. Außerdem ist, wenn du einen Beitrag von jemand anderem kommentierst oder auf dessen Inhalte reagierst, dein Kommentar bzw. deine Reaktion für jeden sichtbar, der die Inhalte der anderen Person sehen kann; darüber hinaus kann eine solche Person später die Zielgruppe ändern.

Personen können unsere Produkte auch nutzen, um Inhalte über dich zu erstellen und sie mit der von ihnen ausgewählten Zielgruppe zu teilen. Beispielsweise können Personen ein Foto von dir in einer Story teilen, dich an einem Standort in einem Beitrag erwähnen oder markieren oder Informationen über dich in ihren Beiträgen oder Nachrichten teilen. Wenn es dir unangenehm ist, was andere über dich auf unseren Produkten geteilt haben, erfährst du hier, wie du Inhalte melden kannst.

Informationen über deinen aktiven Status oder deine Anwesenheit auf unseren Produkten. Personen in deinen Netzwerken können Signale sehen, denen sie entnehmen können, ob du auf unseren Produkten aktiv bist, u. a. ob du gerade aktiv auf Instagram, Messenger oder Facebook bist, oder wann du unsere Produkte zuletzt genutzt hast.

Apps, Websites und Integrationen Dritter, die auf unseren Produkten laufen bzw. diese nutzen.

Wenn du Apps, Webseiten oder sonstige Dienste Dritter verwendest, die unsere Produkte nutzen bzw. über eine Integration mit diesen verfügen, können sie Informationen darüber erhalten, was du postest oder teilst. Wenn du beispielsweise ein Spiel mit deinen Facebook-Freunden/Freundinnen spielst oder einen „Kommentieren“- oder „Teilen“-Button von Facebook auf einer Website verwendest, kann der Spieleentwickler bzw. die Website Informationen über deine Aktivitäten in dem Spiel oder einen Kommentar oder Link erhalten, dass du etwas von der Website auf Facebook teilst. Wenn du solche Drittanbieter-Dienste herunterlädst oder nutzt, können sie auch auf dein öffentliches Profil auf Facebook sowie auf jedwede Informationen, die du mit ihnen teilst, zugreifen. Von dir genutzte Apps und Webseiten können deine Facebook-Freundesliste erhalten, wenn du sie mit ihnen teilst. Allerdings können von dir genutzte Apps und Webseiten keine anderen Informationen von dir über deine Facebook-Freunde oder Informationen über irgendeinen deiner Instagram-Abonnenten erhalten (natürlich können deine Freunde und Abonnenten diese Informationen trotzdem selbst teilen). Die von diesen Diensten Dritter erfassten

Informationen unterliegen deren eigenen Nutzungsbedingungen und Richtlinien und nicht dieser Datenrichtlinie.

Geräte und Betriebssysteme, die native Versionen von Facebook und Instagram bereitstellen (d. h. wenn wir nicht unsere eigenen First-Party-Apps entwickelt haben), haben Zugriff auf sämtliche Informationen, die du mit ihnen teilst, einschließlich der Informationen, die deine Freunde mit dir teilen, damit sie dir unsere Kernfunktionen bereitstellen können.

Hinweis: Zurzeit arbeiten wir daran, den Datenzugriff von Entwicklern noch weiter einzuschränken, um Missbrauch zu verhindern. Beispielsweise werden wir den Zugriff von Entwicklern auf deine Facebook- und Instagram-Daten aufheben, wenn du ihre App 3 Monate lang nicht genutzt hast. Außerdem ändern wir das Login. Somit reduzieren wir in der nächsten Version die Daten, die eine App ohne Überprüfung anfordern kann; es handelt sich dabei dann nur noch um den Namen, den Instagram-Benutzernamen und -Steckbrief, das Profilbild und die E-Mail-Adresse. Für das Anfordern sonstiger Daten ist unsere Genehmigung erforderlich.

Neuer Eigentümer.

Sollten sich die Eigentums- oder Machtverhältnisse aller bzw. eines Teils unserer Produkte oder ihrer Vermögenswerte ändern, können wir deine Informationen an den neuen Eigentümer übertragen.

Teilen mit externen Partnern

Wir arbeiten mit externen Partnern zusammen, die uns dabei unterstützen, unsere Produkte bereitzustellen und zu verbessern, oder die Facebook Business-Tools zur Geschäftssteigerung nutzen. Dies ermöglicht es uns, unsere Unternehmen zu betreiben und den Menschen auf der ganzen Welt kostenlose Dienste bereitzustellen. Wir verkaufen keine deiner Informationen an irgendjemanden und werden das auch in Zukunft niemals tun.

Außerdem legen wir strenge Regeln dafür fest, wie unsere Partner die von uns bereitgestellten Daten verwenden und offenlegen können. Dies sind die Arten Dritter, mit denen wir Informationen teilen:

Partner, die unsere Analysedienste nutzen.

Wir stellen zusammengefasste Statistiken und Einblicke bereit, um Personen und Unternehmen zu helfen, Aufschluss darüber zu erlangen, wie Personen auf und außerhalb von den Facebook-Produkten mit ihren Beiträgen, Kleinanzeigen, Seiten, Videos und sonstigen Inhalten interagieren. Seitenadministratoren und Instagram Business-Profile erhalten z. B. Informationen über die Anzahl der Personen oder Konten, die ihre Beiträge aufgerufen, darauf reagiert oder sie kommentiert haben, sowie zusammengefasste demografische und andere Informationen, die ihnen helfen, etwas über die Interaktionen mit ihrer Seite bzw. ihrem Konto zu erfahren.

Werbetreibende.

Wir stellen Werbetreibenden Berichte über die Arten von Personen, die ihre Werbeanzeigen sehen, und über den Erfolg ihrer Anzeigen bereit, aber wir teilen keine Informationen, die dich persönlich identifizieren (Informationen wie deinen Namen oder deine E-Mail-Adresse, die für sich genommen verwendet werden können, um dich zu kontaktieren oder zu identifizieren), außer du erlaubst uns dies. Wir stellen Werbetreibenden beispielsweise allgemeine demografische und interessenbezogene Informationen bereit (z. B. dass eine Werbeanzeige von einer Frau im Alter zwischen 25 und 34 Jahren, die in Madrid lebt und sich für Software Engineering interessiert, angesehen wurde), um ihnen zu helfen, ihr Publikum besser zu verstehen. Wir bestätigen einem Werbetreibenden außerdem, welche

Facebook-Werbeanzeigen dich dazu veranlasst haben, einen Kauf zu tätigen oder eine Handlung durchzuführen.

Partner für Messungen.

Wir teilen Information über dich mit Unternehmen, die diese zusammenfassen, um unseren Partnern Berichte über Analysen und Messungen bereitzustellen.

Partner, die Waren und Dienstleistungen in unseren Produkten anbieten.

Wenn du den Erhalt von Premium-Inhalten abonnierst oder etwas von einem Verkäufer in unseren Produkten kaufst, kann der Ersteller der Inhalte bzw. der Verkäufer deine öffentlichen Informationen und sonstige Informationen, die du mit ihm teilst, sowie die Informationen erhalten, die zum Abschluss der Transaktion erforderlich sind, einschließlich Versand- und Kontaktangaben.

Anbieter und Dienstleister.

Wir stellen Anbietern und Dienstleistern, die unser Unternehmen unterstützen (z. B. indem sie technische Infrastrukturdienstleistungen erbringen, analysieren, wie unsere Produkte genutzt werden, einen Kundendienst anbieten, Zahlungen ermöglichen oder Umfragen durchführen), Informationen und Inhalte bereit.

Forscher und Wissenschaftler.

Außerdem stellen wir Informationen und Inhalte für Forschungspartner und Wissenschaftler bereit, damit diese Recherchen durchführen können, die Forschung und Innovation zur Unterstützung unseres Unternehmens bzw. unserer Mission vorantreiben und Entdeckung und Innovation zu Themen des sozialen Allgemeinwohls, des technologischen Fortschritts, des öffentlichen Interesses, der Gesundheit und des Wohlergehens verbessern.

Strafverfolgungs- bzw. Vollstreckungsbehörden oder rechtliche Anfragen.

Wir teilen Informationen mit Strafverfolgungsbehörden oder als Reaktion auf rechtliche Anfragen unter den weiter unten dargelegten Umständen.

In den Facebook-Einstellungen und den Instagram-Einstellungen erfährst du mehr darüber, wie du die Informationen über dich kontrollieren kannst, die du mit Drittpartnern teilst bzw. andere mit diesen teilen.

IV. Wie arbeiten die Facebook-Unternehmen zusammen?

Facebook und Instagram teilen die Infrastruktur, die Systeme und die Technologie mit anderen Facebook-Unternehmen (dies sind u. a. WhatsApp und Oculus), um ein innovatives, relevantes, einheitliches und sicheres Erlebnis auf allen von dir genutzten Produkten der Facebook-Unternehmen bereitzustellen. Für diese Zwecke verarbeiten wir Informationen über dich auch über die Facebook-Unternehmen hinweg, soweit dies nach geltendem Recht und gemäß deren Nutzungsbedingungen und Richtlinien zulässig ist. Beispielsweise verarbeiten wir Informationen von WhatsApp bezüglich Konten, die Spam auf dem Dienst versenden, damit wir geeignete Maßnahmen gegen solche Konten auf Facebook, auf Instagram oder im Messenger ergreifen können. Außerdem versuchen wir herauszufinden, wie Personen Produkte der Facebook-Unternehmen nutzen und mit ihnen interagieren, beispielsweise um Aufschluss über die Anzahl der individuellen Nutzer auf verschiedenen Produkten der Facebook-Unternehmen zu erhalten.

V. Was ist unsere Rechtsgrundlage für die Verarbeitung von Daten?

Wir erfassen, verwenden und teilen die uns zur Verfügung stehenden Daten auf die oben beschriebenen Arten:

wie es zur Einhaltung unserer Facebook-Nutzungsbedingungen oder der Instagram-Nutzungsbedingungen erforderlich ist;
gemäß deiner Einwilligung, die du jederzeit über die Facebook-Einstellungen und die Instagram-Einstellungen widerrufen kannst;
wie es zur Erfüllung unserer rechtlichen Pflichten erforderlich ist;
um deine wesentlichen Interessen oder die von anderen zu schützen;
wie es im öffentlichen Interesse erforderlich ist; und
wie es für unsere berechtigten Interessen (sowie die von anderen) erforderlich ist, einschließlich unseres Interesses daran, innovative, personalisierte, sichere und profitable Dienste für unsere Nutzer und Partner bereitzustellen, außer wenn diese Interessen von deinen Interessen oder grundlegenden Rechten und Freiheiten, die den Schutz personenbezogener Daten erfordern, überwogen werden.
Erfahre mehr über diese Rechtsgrundlagen und wie diese mit den Arten und Weisen, auf die wir Daten verarbeiten, im Zusammenhang stehen.

VI. Wie kannst du deine gemäß DSGVO gewährten Rechte ausüben?

Gemäß Datenschutz-Grundverordnung hast du das Recht auf Auskunft, Berichtigung, Übertragbarkeit und Löschung deiner Daten. Erfahre mehr über diese Rechte und finde heraus, wie du deine Rechte in den Facebook-Einstellungen und Instagram-Einstellungen ausüben kannst. Du hast auch das Recht Widerspruch einzulegen gegen bestimmte Verarbeitungen deiner Daten bzw. sie einzuschränken. Dazu gehören:
das Recht, Widerspruch gegen unsere Verarbeitung deiner Daten für Direktwerbung einzulegen, welches du durch Verwendung des „Abbestellen“-Links in solchen Marketing-Kommunikationen ausüben kannst, und
das Recht, Widerspruch gegen unsere Verarbeitung deiner Daten in dem Fall einzulegen, wenn wir eine Aufgabe im öffentlichen Interesse erfüllen oder unsere berechtigten Interessen bzw. die eines Dritten verfolgen. Du kannst dieses Recht auf Facebook und auf Instagram ausüben.

VII. Datenspeicherung, Deaktivierung und Löschung von Konten

Wir speichern Daten, bis sie nicht mehr benötigt werden, um unsere Dienste und Facebook-Produkte bereitzustellen, oder bis dein Konto gelöscht wird, je nachdem, was zuerst eintritt. Dies ist eine Einzelfallbestimmung und hängt von Dingen ab wie der Art der Daten, warum sie erfasst und verarbeitet werden sowie den relevanten rechtlichen oder betrieblichen Speicherbedürfnissen. Wenn du beispielsweise nach etwas auf Facebook suchst, kannst du auf diese Anfrage jederzeit aus deinem Suchverlauf zugreifen und sie löschen; allerdings wird das Protokoll dieser Suche erst nach 6 Monaten gelöscht. Wenn du eine Kopie deines amtlichen Ausweises zur Kontoverifizierung einreichst, löschen wir diese Kopie 30 Tage nach der Prüfung, sofern nicht anders angegeben. Erfahre mehr über die Löschung von Inhalten, die du geteilt hast, und über Cookie-Daten, die über soziale Plugins erhalten wurden. Wenn du dein Konto löschst, löschen wir von dir gepostete Dinge, wie beispielsweise deine Fotos und Status-Updates, und diese Informationen kannst du anschließend nicht wiederherstellen. Informationen, die andere über dich geteilt haben, gehören nicht zu deinem Konto und werden nicht gelöscht. Falls du dein Konto nicht löschen, sondern deine Nutzung der Produkte lediglich vorübergehend beenden möchtest, kannst du dein Konto stattdessen deaktivieren. Um dein Konto zu löschen, gehe bitte immer zu den Facebook-Einstellungen und den Instagram-Einstellungen.

VIII. Wie reagieren wir auf rechtliche Anfragen bzw. wie verhindern wir Schäden?

Wir greifen auf deine Informationen zu, bewahren sie auf und teilen sie mit Aufsichts-, Strafverfolgungs- oder anderen Behörden:

Als Reaktion auf eine rechtliche Anfrage, wenn wir in gutem Glauben der Ansicht sind, dass wir rechtlich hierzu verpflichtet sind. Wir können auch auf rechtliche Anfragen reagieren, wenn wir in gutem Glauben der Ansicht sind, dass die Reaktion nach dem Recht der betreffenden Gerichtsbarkeit vorgeschrieben ist, Nutzer in der betreffenden Gerichtsbarkeit betrifft und mit international anerkannten Standards vereinbar ist.

Wenn wir in gutem Glauben der Ansicht sind, dass es für Folgendes erforderlich ist: Um Betrug, eine unberechtigte Nutzung der Produkte, Verstöße gegen unsere Nutzungsbedingungen und Richtlinien sowie sonstige schädliche oder illegale Aktivitäten aufzudecken, zu verhindern und zu verfolgen; um uns (einschließlich unserer Rechte, unseres Eigentums oder unserer Produkte), dich oder andere zu schützen, u. a. im Rahmen von Untersuchungen oder Auskunftersuchen der Aufsichtsbehörden; oder um den Tod oder eine drohende Körperverletzung zu verhindern. Zum Beispiel werden wir, falls relevant, Drittpartnern Informationen über die Vertrauenswürdigkeit deines Kontos zur Verfügung stellen und von ihnen erhalten, um Betrug, Missbrauch und sonstige schädliche Aktivitäten auf und außerhalb von unseren Produkten zu verhindern.

Auf Informationen, die wir über dich erhalten (einschließlich Daten zu finanziellen Transaktionen im Zusammenhang mit über Facebook getätigten Käufen), kann über einen längeren Zeitraum zugriffen bzw. können diese länger aufbewahrt werden, wenn sie Gegenstand einer Anfrage oder Pflicht rechtlicher Art, behördlichen Untersuchung oder Untersuchungen möglicher Verstöße gegen unsere Nutzungsbedingungen oder Richtlinien sind, oder um auf sonstige Weise Schaden zu verhindern. Wir speichern außerdem mindestens ein Jahr lang Informationen über Konten, die aufgrund von Verstößen gegen Nutzungsbedingungen deaktiviert worden sind, um einen wiederholten Missbrauch oder sonstige Verstöße gegen Nutzungsbedingungen zu verhindern.

IX. Wie verarbeiten und übermitteln wir Daten im Rahmen unserer globalen Dienste?

Wir teilen Informationen weltweit, sowohl intern zwischen den Facebook-Unternehmen als auch extern mit unseren Partnern sowie mit denen, mit denen du dich auf der ganzen Welt verbindest und mit denen du etwas teilst, im Einklang mit dieser Richtlinie. Deine von Facebook Ireland kontrollierten Informationen werden für die in dieser Richtlinie beschriebenen Zwecke in die USA oder andere Drittländer übertragen oder übermittelt bzw. dort gespeichert und verarbeitet. Diese Datenübermittlungen sind erforderlich, um die in den Facebook-Nutzungsbedingungen und Instagram-Nutzungsbedingungen dargelegten Dienste bereitzustellen und um global tätig zu sein und dir unsere Produkte bereitzustellen. Wir verwenden von der Europäischen Kommission genehmigte Standardvertragsklauseln und verlassen uns für Datenübermittlungen aus dem EWR in die USA und andere Länder ggf. auf die von der Europäischen Kommission erlassenen Angemessenheitsbeschlüsse bezüglich bestimmter Länder.

X. Wie benachrichtigen wir dich über Änderungen an dieser Richtlinie?

Wir benachrichtigen dich, bevor wir Änderungen an dieser Richtlinie vornehmen, und geben dir die Gelegenheit, die überarbeitete Richtlinie zu überprüfen, bevor du dich dazu entscheidest, unsere Produkte weiterhin zu nutzen.

XI. So kontaktierst du Facebook bei Fragen

Weitere Informationen zur Funktionsweise des Datenschutzes findest du auf Facebook und auf Instagram. Solltest du Fragen zu dieser Richtlinie haben, kannst du uns wie unten beschrieben kontaktieren.

Der Datenverantwortliche bezüglich deiner Informationen ist Facebook Ireland. Dieses Unternehmen kannst du entweder online kontaktieren oder per Post an:

Facebook Ireland Ltd.
4 Grand Canal Square
Grand Canal Harbour
Dublin 2 Ireland

Kontaktaufnahme mit dem Datenschutzbeauftragten für Facebook Ireland Ltd.

Du hast außerdem das Recht, eine Beschwerde bei der für Facebook Ireland zuständigen führenden Aufsichtsbehörde, der irischen Datenschutzkommission, oder bei deiner lokalen Aufsichtsbehörde einzureichen.

Datum der letzten Überarbeitung: 21. August 2020

Haupt-Cluster	Nr.	Bezeichnung Richtlinien	ID1	ID2	ID3	ID4	ID5	ID6	ID7
Cluster 4	1	Mobilfunkanbieter	Geräte-Daten	Technische Daten	Geräte-Daten	Technische Daten;	Geräte-Daten	Mobil-Daten	Technische Daten
Cluster 4	2	Geräte-ID	Geräte-Daten	Technische Daten	Geräte-Daten	Technische Daten	Geräte-Daten	Mobil-Daten	Technische Daten
Cluster 3	3	Name	Persönliche Daten	Persönliche Daten	Kontaktdaten	Anschrift-Daten	Allgemeine Daten	Kontakt-Daten	Personen-Daten
Cluster 3	4	E-Mailadresse	Persönliche Daten	Persönliche Daten	Kontaktdaten	Anschrift-Daten	Allgemeine Daten	Kontakt-Daten	Personen-Daten
Cluster 3	5	Wohnort	Persönliche Daten	Persönliche Daten	Kontaktdaten	Anschrift-Daten	Allgemeine Daten	Kontakt-Daten	Personen-Daten
Cluster 3	6	Alter	Persönliche Daten	Persönliche Daten	Kontaktdaten	Persönliche Daten	Allgemeine Daten	Kontakt-Daten	Personen-Daten
Cluster 3	7	Geburtsdatum	Persönliche Daten	Persönliche Daten	Kontaktdaten	Persönliche Daten	Allgemeine Daten	Kontakt-Daten	Personen-Daten
Cluster 2	8	Gesichtserkennung	Überwachungsdaten	Private Daten	Überwachungsdaten	Höchstpersönliche Daten	Private Daten	Persönliche Daten	Personen-Daten
Cluster 4	9	Besuchte Webseiten	Überwachungsdaten	Technische Daten	Überwachungsdaten	Technische Daten	Private Daten	Bewegungs-Daten	Nutzungs-Daten
Cluster 2	10	Persönliches Adressbuch	Private Daten	Persönliche Daten	Überwachungsdaten	Persönliche Daten	Private Daten	Persönliche Daten	Personen-Daten
Cluster 4	11	Geo-Tag	User-Aktion	Ortungs-Daten	Überwachungsdaten	Standortdaten	Geräte-Daten	Bewegungs-Daten	Standort-Daten
Cluster 2	12	Zahlungsinformation	Private Daten	Persönliche Daten	Überwachungsdaten	Persönliche Daten	Private Daten	Persönliche Daten	Technische Daten
Cluster 2	13	Gesendete Nachrichten	User-Interaktion	Private Daten	Überwachungsdaten	Persönliche Daten	Private Daten	Persönliche Daten	Nutzungs-Daten
Cluster 2	14	Chatnachrichten	User-Interaktion	Private Daten	Überwachungsdaten	Persönliche Daten	Private Daten	Mobil-Daten	Nutzungs-Daten
Cluster 2	15	Anrufprotokoll	Überwachungsdaten	Private Daten	Überwachungsdaten	Persönliche Daten	Geräte-Daten	Mobil-Daten	Technische Daten
Cluster 4	16	Gespeicherte Cookies	Überwachungsdaten	Technische Daten	Überwachungsdaten	Technische Daten	Geräte-Daten	Geräte-Daten	Technische Daten
Cluster 4	17	GPS-Standort	Überwachungsdaten	Ortungs-Daten	Überwachungsdaten	Standortdaten	Geräte-Daten	Bewegungs-Daten	Standort-Daten
Cluster 2	18	Persönliche Nachrichten	User-Interaktion	Private Daten	Überwachungsdaten	Persönliche Daten	Private Daten	Aktions-Daten	Nutzungs-Daten
Cluster 2	19	Kaufverhalten	User-Gruppierung	Private Daten	Überwachungsdaten	Persönliche Daten	Private Daten	Persönliche Daten	Nutzungs-Daten
Cluster 1	20	Nutzername	User-Aktion	Profil-Daten	Profil-Daten	Profil-Daten	Plattform-Daten	Profil-Daten	Nutzungs-Daten
Cluster 1	21	Kontakte	Private Daten	Profil-Daten	Profil-Daten	Profil-Daten	Plattform-Daten	Profil-Daten	Nutzungs-Daten
Cluster 1	22	Freunde	User-Interaktion	Profil-Daten	Profil-Daten	Profil-Daten	Plattform-Daten	Profil-Daten	Nutzungs-Daten
Cluster 1	23	Beiträge/Postings	User-Aktion	Profil-Daten	Profil-Daten	Profil-Daten	Plattform-Daten	Aktions-Daten	Nutzungs-Daten
Cluster 1	24	Verweildauer	Überwachungsdaten	Profil-Daten	Profil-Daten	Technische Daten	Geräte-Daten	Geräte-Daten	Nutzungs-Daten
Cluster 1	25	#Hashtags	User-Aktion	Profil-Daten	Profil-Daten	Profil-Daten	Plattform-Daten	Aktions-Daten	Nutzungs-Daten
Cluster 1	26	Likes	User-Interaktion	Profil-Daten	Profil-Daten	Profil-Daten	Plattform-Daten	Aktions-Daten	Nutzungs-Daten
Cluster 1	27	Reaktionen (Emojis)	User-Interaktion	Profil-Daten	Profil-Daten	Profil-Daten	Plattform-Daten	Aktions-Daten	Nutzungs-Daten
Cluster 1	28	Profil-Foto	User-Aktion	Profil-Daten	Profil-Daten	Profil-Daten	Plattform-Daten	Profil-Daten	Nutzungs-Daten
Cluster 1	29	Hochgeladene Files/Videos	User-Aktion	Profil-Daten	Profil-Daten	Profil-Daten	Plattform-Daten	Aktions-Daten	Nutzungs-Daten
Cluster 1	30	Follower	User-Interaktion	Profil-Daten	Profil-Daten	Profil-Daten	Plattform-Daten	Profil-Daten	Nutzungs-Daten
Cluster 1	31	Interaktionen	User-Interaktion	Profil-Daten	Profil-Daten	Profil-Daten	Plattform-Daten	Aktions-Daten	Nutzungs-Daten
Cluster 1	32	Markierungen (Tags)	User-Interaktion	Profil-Daten	Profil-Daten	Profil-Daten	Plattform-Daten	Aktions-Daten	Nutzungs-Daten
Cluster 1	33	Gruppen (öffentlich/privat)	User-Interaktion	Profil-Daten	Profil-Daten	Profil-Daten	Plattform-Daten	Aktions-Daten	Nutzungs-Daten
Cluster 1	34	Kommentare	User-Interaktion	Profil-Daten	Profil-Daten	Profil-Daten	Plattform-Daten	Aktions-Daten	Nutzungs-Daten
Cluster 2	35	Gesundheitsdaten	Private Daten	Private Daten	Sensible Daten	Höchstpersönliche Daten	Private Daten	Persönliche Daten	Personen-Daten
Cluster 2	36	Sexuelle Orientierung	Private Daten	Private Daten	Sensible Daten	Höchstpersönliche Daten	Private Daten	Persönliche Daten	Personen-Daten
Cluster 2	37	Biometrische Daten	Überwachungsdaten	Private Daten	Sensible Daten	Höchstpersönliche Daten	Private Daten	Persönliche Daten	Personen-Daten
Cluster 4	38	Genutzte Geräte	Überwachungsdaten	Technische Daten	Geräte-Daten	Technische Daten	Geräte-Daten	Geräte-Daten	Technische Daten
Cluster 4	39	Telefonmarke	Geräte-Daten	Technische Daten	Geräte-Daten	Technische Daten	Geräte-Daten	Mobil-Daten	Technische Daten
Cluster 4	40	TelefonEinstellungen	Geräte-Daten	Technische Daten	Geräte-Daten	Technische Daten	Geräte-Daten	Mobil-Daten	Technische Daten
Cluster 4	41	Verwendetes Betriebssystem	Überwachungsdaten	Technische Daten	Geräte-Daten	Technische Daten	Geräte-Daten	Geräte-Daten	Technische Daten
Cluster 4	42	IP-Adresse	Private Daten	Technische Daten	Geräte-Daten	Technische Daten	Geräte-Daten	Geräte-Daten	Technische Daten
Cluster 3	43	Nationalität	Persönliche Daten	Persönliche Daten	Persönliche Daten	Persönliche Daten	Allgemeine Daten	Persönliche Daten	Personen-Daten
Cluster 3	44	Interessen	User-Gruppierung	Persönliche Daten	Persönliche Daten	Persönliche Daten	Allgemeine Daten	Persönliche Daten	Personen-Daten
Cluster 3	45	Geschlecht	Persönliche Daten	Persönliche Daten	Persönliche Daten	Persönliche Daten	Allgemeine Daten	Kontakt-Daten	Personen-Daten
Cluster 3	46	Beruf	Persönliche Daten	Persönliche Daten	Persönliche Daten	Persönliche Daten	Allgemeine Daten	Kontakt-Daten	Personen-Daten
Cluster 2	47	Politische Ansichten	User-Gruppierung	Private Daten	Persönliche Daten	Persönliche Daten	Private Daten	Persönliche Daten	Interessens-Daten
Cluster 2	48	Religiöse Ansichten	Private Daten	Private Daten	Persönliche Daten	Persönliche Daten	Private Daten	Persönliche Daten	Interessens-Daten
Cluster 2	49	Gewerkschaftszugehörigkeit	Private Daten	Private Daten	Persönliche Daten	Persönliche Daten	Private Daten	Persönliche Daten	Interessens-Daten
Cluster 3	50	Ethnische Herkunft	Private Daten	Private Daten	Persönliche Daten	Persönliche Daten	Private Daten	Persönliche Daten	Personen-Daten

ID18	ID19	ID20
Telefon-Daten	Anbieter-Daten	Geräte-Daten
Telefon-Daten	Hersteller-Daten	Geräte-Daten
Personen-Daten	Adress-Daten	Persönliche Daten
Personen-Daten	Adress-Daten	Persönliche Daten
Ortungs-Daten	Adress-Daten	Persönliche Daten
Personen-Daten	Personen-Daten	Persönliche Daten
Personen-Daten	Personen-Daten	Persönliche Daten
Sensible Daten	Private Daten	Sensible Daten
Ortungs-Daten	Technische Daten	Nutzerverhalten
Personen-Daten	Private Daten	Persönliche Daten
Ortungs-Daten	Überwachungs-Daten	Tracking-Daten
Sensible Daten	Bank-Daten	Persönliche Daten
Nutzungs-Daten	Private Daten	Nutzerverhalten
Nutzungs-Daten	Private Daten	Nutzerverhalten
Nutzungs-Daten	Private Daten	Nutzerverhalten
Ortungs-Daten	Überwachungs-Daten	Nutzerverhalten
Ortungs-Daten	Überwachungs-Daten	Tracking-Daten
Nutzungs-Daten	Private Daten	Nutzerverhalten
Sensible Daten	Private Daten	Nutzerverhalten
Nutzungs-Daten	Plattform-Daten	Profil-Daten
Nutzungs-Daten	Plattform-Daten	Profil-Daten
Nutzungs-Daten	Plattform-Daten	Profil-Daten
Nutzungs-Daten	Plattform-Daten	Nutzerverhalten
Nutzungs-Daten	Plattform-Daten	Nutzerverhalten
Nutzungs-Daten	Plattform-Daten	Nutzerverhalten
Nutzungs-Daten	Plattform-Daten	Nutzerverhalten
Nutzungs-Daten	Plattform-Daten	Nutzerverhalten
Nutzungs-Daten	Plattform-Daten	Profil-Daten
Nutzungs-Daten	Plattform-Daten	Nutzerverhalten
Nutzungs-Daten	Plattform-Daten	Profil-Daten
Nutzungs-Daten	Plattform-Daten	Nutzerverhalten
Ortungs-Daten	Plattform-Daten	Nutzerverhalten
Nutzungs-Daten	Plattform-Daten	Nutzerverhalten
Nutzungs-Daten	Plattform-Daten	Nutzerverhalten
Sensible Daten	Private Daten	Sensible Daten
Sensible Daten	Private Daten	Sensible Daten
Sensible Daten	Private Daten	Sensible Daten
Geräte-Daten	Geräte-Daten	Geräte-Daten
Geräte-Daten	Hersteller-Daten	Geräte-Daten
Geräte-Daten	Hersteller-Daten	Nutzerverhalten
Geräte-Daten	Hersteller-Daten	Geräte-Daten
Ortungs-Daten	Geräte-Daten	Geräte-Daten
Personen-Daten	Adress-Daten	Persönliche Daten
Personen-Daten	Personen-Daten	Persönliche Daten
Personen-Daten	Personen-Daten	Persönliche Daten
Personen-Daten	Personen-Daten	Persönliche Daten
Sensible Daten	Private Daten	Sensible Daten
Sensible Daten	Private Daten	Sensible Daten
Sensible Daten	Private Daten	Sensible Daten
Sensible Daten	Personen-Daten	Sensible Daten

Label	ID1	ID2	ID3	ID4	ID5	ID6	ID7	ID8	ID9	ID10	ID11	ID12	ID13	ID14	ID15	ID16	ID17	ID18	ID19	ID20
1	a	c	a	c	a	b	c	a	a	c	c	a	g1	c	a	c	c	g1	j1	a
2	a	c	a	c	a	b	c	x	a	c	a1	a	g1	c	a	c	c	g1	d	a
3	f	f	h	j	g	h	i	e	f	k	h	c1	i	i	i	j	e	i	l	f
4	f	f	h	j	g	h	i	e	f	h	h	c1	l	i	i	j	e	i	l	f
5	f	f	h	j	g	h	i	e	f	h	h	a1	l	i	i	j	e	v	l	f
6	f	f	h	f	g	h	i	e	f	k	i	m	i	i	i	f	e	i	i	f
7	f	f	h	f	g	h	i	e	f	k	i	c1	i	i	i	j	e	i	i	f
8	a1	b1	a1	d1	b1	f	i	c1	c1	k	a1	a1	f1	b1	c1	f	c1	c1	b1	c1
9	a1	c	a1	c	b1	z	q	x	n1	q	a1	a1	c	a1	x	c	e	v	c	k1
10	b1	f	a1	f	b1	f	i	e	f	f	i	u	g1	u	c1	f	e	i	b1	f
11	s	v	a1	y	a	z	y	x	n1	c	a1	a1	y	a1	w	y	x	v	a1	x
12	b1	f	a1	f	b1	f	c	c1	c1	it	p1	c1	h1	b1	c1	f	e	c1	h1	f
13	n	b1	a1	f	b1	f	q	r	n1	q	e1	u	f1	u	o	f	m1	q	b1	k1
14	n	b1	a1	f	b1	b	q	r	n1	q	e1	u	f1	u	o	f	m1	q	b1	k1
15	a1	b1	a1	f	a	b	c	r	n1	q	e1	u	g1	u	a	f	m1	q	b1	k1
16	a1	c	a1	c	a	a	c	r	n1	c	a1	a1	c	a1	x	c	e	v	a1	k1
17	a1	v	a1	y	a	z	y	x	n1	c	a1	a1	y	a1	w	y	x	v	a1	x
18	n	b1	a1	f	b1	p	q	r	f	q	e1	u	f1	u	c1	f	m1	q	b1	k1
19	o1	b1	a1	f	b1	f	q	r	f	q	a1	m	f1	b1	x	f	m1	c1	b1	k1
20	s	m	m	m	o	m	q	m	m	m	o	m	m	m	o	f	m1	q	o	m
21	b1	m	m	m	o	m	q	m	f	m	o	u	m	m	a	f	m1	q	o	m
22	n	m	m	m	o	m	q	m	m	m	o	m	m	m	o	f	m1	q	o	m
23	s	m	m	m	o	p	q	r	n1	q	o	t	m	t	o	f	m1	q	o	k1
24	a1	m	m	c	a	a	q	r	n1	c	o	m	c	c	a	c	x	q	o	k1
25	s	m	m	m	o	p	q	r	n1	q	o	t	m	t	o	o	m1	q	o	k1
26	n	m	m	m	o	p	q	r	n1	q	o	t	m	t	o	o	m1	q	o	k1
27	n	m	m	m	o	p	q	r	n1	q	o	t	m	t	o	o	m1	q	o	k1
28	s	m	m	m	o	m	q	m	m	m	o	m	m	m	o	f	m1	q	o	m
29	s	m	m	m	o	p	q	r	n1	q	o	m	m	t	o	f	m1	q	o	k1
30	n	m	m	m	o	m	q	m	m	q	o	m	m	m	o	o	m1	q	o	m
31	n	m	m	m	o	p	q	r	n1	q	o	t	m	t	o	o	m1	q	o	k1
32	n	m	m	m	o	p	q	r	n1	q	o	a1	m	t	o	o	x	v	o	k1
33	n	m	m	m	o	p	q	m	m	q	o	t	m	t	o	o	m1	q	o	k1
34	n	m	m	m	o	p	q	r	n1	q	o	t	m	t	o	o	m1	q	o	k1
35	b1	b1	c1	d1	b1	f	i	c1	c1	f	e1	c1	f1	b1	c1	b1	c1	c1	b1	c1
36	b1	b1	c1	d1	b1	f	i	c1	f	f	e1	c1	i	b1	c1	b1	c1	c1	b1	c1
37	a1	b1	c1	d1	b1	f	i	c1	c1	f	e1	c1	i	b1	c1	b1	c1	c1	b1	c1
38	a1	c	a	c	a	a	c	a	a	a	a1	a	a	c	a	c	m1	a	c	a
39	a	c	a	c	a	b	c	a	a	a	c	a	g1	c	a	c	c	a	d	a
40	a	c	a	c	a	b	c	a	a	c	c	a	g1	c	a	c	c	a	d	k1
41	a1	c	a	c	a	a	c	a	a	c	c	a	c	c	a	c	c	a	d	a
42	b1	c	a	c	a	a	c	x	a	c	a1	a	c	b1	a	c	e	v	c	a
43	f	f	f	f	g	f	i	e	f	k	i	c1	i	i	i	j	e	i	l	f
44	o1	f	f	f	g	f	i	e	f	m	i	m	i	i	i	f	e	i	i	f
45	f	f	f	f	g	h	i	e	f	k	i	c1	i	i	i	f	e	i	i	f
46	f	f	f	f	g	h	i	e	f	h	i	m	i	i	i	f	e	i	i	f
47	o1	b1	f	f	b1	f	l1	c1	f	f	i	c1	f1	b1	c1	b1	c1	c1	b1	c1
48	b1	b1	f	f	b1	f	l1	c1	f	f	i	c1	i	b1	c1	b1	c1	c1	b1	c1
49	b1	b1	f	f	b1	f	l1	c1	f	f	i	c1	f1	b1	i	b1	c1	c1	b1	c1
50	b1	b1	f	f	b1	f	i	e	f	k	i	c1	i	i	i	f	c1	c1	i	c1

Nutzer innen_Kategorien	Wert	Anzahl Einträge
Geräte-Daten	a	61
Mobil-Daten	b	6
Technische Daten	c	72
Hersteller-Daten	d	4
Personenbezogene Daten	e	26
Persönliche Daten	f	113
Allgemeine Daten	g	9
Kontakt-Daten	h	18
Personen-Daten	i	73
Anschrift-Daten	j	8
Identitäts-Daten	k	7
Adress-Daten	l	6
Profil-Daten	m	99
User-Interaktion	n	11
Plattform-Daten	o	67
Aktions-Daten	p	10
Nutzungs-Daten	q	54
Verhaltensbezogene Daten	r	15
User-Aktion	s	6
Öffentliche Kommunikation	t	16
Private Kommunikation	u	11
Ortungs-Daten	v	9
Orts-Daten	w	2
Tracking-Daten	x	14
Standort-Daten	y	8
Bewegungs-Daten	z	3
Überwachungs-Daten	a1	44
Private Daten	b1	66
Sensible Daten	c1	63
Höchstpersönliche Daten	d1	4
Empfindliche Daten	e1	7
Geheime Daten	f1	8
Telefon-Daten	g1	8
Bank-Daten	h1	2
Finanzdaten	i1	1
Anbieter-Daten	j1	1
Nutzerverhalten	k1	18
Interessens-Daten	l1	3
Interaktions-Daten	m1	19
Verhaltens-Daten	n1	16
User-Gruppierung	o1	3
Zahlungsdaten	p1	1

Bezeichnung Richtlinien

Mobilfunkanbieter, Geräte-ID, Telefon-Marke, Telefon-Einstellungen, Genutzte Geräte, Verwendetes Betriebssystem, IP-Adresse, Geo-Tag, Anrufprotokoll, Gespeicherte Cookies, GPS-Standort, Verweildauer, Kontakte

Mobilfunkanbieter, Geräte-ID, Chatnachrichten, Anrufprotokoll, Genutzte Geräte, Telefonmarke

Mobilfunkanbieter, Geräte-ID, Gesichtserkennung, Gespeicherte Cookies, Genutzte Geräte, Telefonmarke, Telefon-Einstellungen, Verwendetes Betriebssystem, IP-Adresse, Verweildauer, Zahlungsinformation, Anrufprotokoll, Geo-Tag, GPS-Standort

Geräte-ID, Telefoneinstellungen, Verwendetes Betriebssystem, IP-Adresse

Name, E-Mailadresse, Wohnort, Alter, Geburtsdatum, Persönliches Adressbuch, Nationalität, Interessen, Geschlecht, Beruf, Ethnische Herkunft, Besuchte Webseiten, Zahlungsinformation, Gespeicherte Cookies, IP-Adresse

Name, E-Mailadresse, Wohnort, Alter, Geburtsdatum, Nationalität, Geschlecht, Beruf, Persönliches Adressbuch, Zahlungsinformation, Interessen, Politische Ansichten, Religiöse Ansichten, Gewerkschaftszugehörigkeit, Ethnische Herkunft, Gesendete Nachr

Persönliche Nachrichten, Kaufverhalten, Gesichtserkennung, Gesundheitsdaten, Sexuelle Orientierung, Biometrische Daten, Kontakte, Nutzernamen, Freunde, Beiträge/Postings, Profil-Foto, Hochgeladene Files/Videos

Name, E-Mailadresse, Wohnort, Alter, Geburtsdatum, Nationalität, Interessen, Geschlecht, Beruf

Name, E-Mailadresse, Wohnort, Alter, Geburtsdatum, Geschlecht, Beruf

Name, E-Mailadresse, Wohnort, Alter, Geburtsdatum, Gesichtserkennung, Persönliches Adressbuch, Gesundheitsdaten, Sexuelle Orientierung, Biometrische Daten, Nationalität, Interessen, Geschlecht, Beruf, Ethnische Herkunft, Politische Ansichten, Religiö

Name, E-Mailadresse, Wohnort, Geburtsdatum, Nationalität

Name, Alter, Geburtsdatum, Gesichtserkennung, Nationalität, Geschlecht, Ethnische Herkunft

E-Mailadresse, Wohnort, Name, Nationalität

Nutzername, Kontakte, Freunde, Beiträge/Postings, Verweildauer, # Hashtags, Likes, Reaktionen (Emojis), Profil-Foto, Hochgeladene Files/Videos, Follower, Interaktionen, Markierungen (Tags), Gruppen (öffentlich/privat), Kommentare, Geschlecht, Alter, Kau

Gesendete Nachrichten, Chatnachrichten, Persönliche Nachrichten, Freunde, Likes, Reaktionen (Emojis), Follower, Interaktionen, Markierungen (Tags), Gruppen (öffentlich/privat), Kommentare

Nutzername, Kontakte, Freunde, Beiträge/Postings, Verweildauer, # Hashtags, Likes, Reaktionen (Emojis), Profil-Foto, Hochgeladene Files/Videos, Follower, Interaktionen, Markierungen (Tags), Gruppen (öffentlich/privat), Kommentare, Gesendete Nachrichte

Persönliche Nachrichten, Beiträge/Postings, # Hashtags, Likes, Reaktionen (Emojis), Hochgeladene Files/Videos, Interaktionen, Markierungen (Tags), Gruppen (öffentlich/privat), Kommentare

Besuchte Webseiten, Gesendete Nachrichten, Chatnachrichten, Persönliche Nachrichten, Kaufverhalten, Nutzernamen, Kontakte, Freunde, Beiträge/Postings, Verweildauer, # Hashtags, Likes, Reaktionen (Emojis), Profil-Foto, Hochgeladene Files/Videos, Foll

Gruppen (öffentlich/privat), Kommentare, Anrufprotokoll

Gesendete Nachrichten, Chatnachrichten, Anrufprotokoll, Gespeicherte Cookies, Beiträge/Postings, Verweildauer, # Hashtags, Likes, Reaktionen (Emojis), Hochgeladene Files/Videos, Interaktionen, Markierungen (Tags), Kommentare, Persönliche Nachrichte

Geo-Tag, Nutzer-Name, Beiträge/Postings, #Hashtags, Profil-Foto, Hochgeladene Files/Videos

Beiträge/Postings, #Hashtags, Likes, Reaktionen (Emojis), Interaktionen, Gruppen (öffentlich/privat), Kommentare, Hochgeladene Files/Videos, Markierungen (Tags)

Persönliches Adressbuch, Gesendete Nachrichten, Chatnachrichten, Anrufprotokoll, Persönliche Nachrichten, Kontakte

Geo-Tag, GPS-Standort, Wohnort, Besuchte Webseiten, Persönliche Nachrichten, Markierungen (Tags), IP-Adresse

Geo-Tag, GPS-Standort

Geräte-ID, Besuchte Webseiten, Geo-Tag, GPS-Standort, IP-Adresse, Gespeicherte Cookies, Kaufverhalten, Verweildauer, Markierungen (Tags)

Geo-Tag, GPS-Standort

Besuchte Webseiten, Geo-Tag, GPS-Standort

Gesichtserkennung, Besuchte Webseiten, Anrufprotokoll, Gespeicherte Cookies, GPS-Standort, Verweildauer, Biometrische Daten, Genutzte Geräte, Verwendetes Betriebssystem, Persönliches Adressbuch, Geo-Tag, Zahlungsinformation, Gesendete Nachr

Gespeicherte Cookies, Persönliche Nachrichten, Kaufverhalten, Geräte ID, IP-Adresse, Wohnort, Markierungen (Tags)

Persönliches Adressbuch, Zahlungsinformation, Kontakte, Gesundheitsdaten, Sexuelle Orientierung, IP-Adresse, Religiöse Ansichten, Gewerkschaftszugehörigkeit, Ethnische Herkunft, Gesichtserkennung, Gesendete Nachrichten, Chatnachrichtenn Anrufpr

Biometrische Daten, Politische Ansichten, Besuchte Webseiten,

Gesundheitsdaten, Sexuelle Orientierung, Biometrische Daten, Gesichtserkennung, Zahlungsinformation, Politische Ansichten, Religiöse Ansichten, Gewerkschaftszugehörigkeit, Name, E-Mailadresse, Nationalität, Geschlecht, Ethnische Herkunft, Persönliche

Gesichtserkennung, Gesundheitsdaten, Sexuelle Orientierung, Biometrische Daten

Gesendete Nachrichten, Chatnachrichten, Anrufprotokoll, Persönliche Nachrichten, Gesundheitsdaten, Sexuelle Orientierung, Biometrische Daten

Gesichtserkennung, Gesendete Nachrichten, Chatnachrichten, Persönliche Nachrichten, Kaufverhalten, Gesundheitsdaten, Politische Ansichten, Gewerkschaftszugehörigkeit,

Mobilfunkanbieter, Geräte-ID, Persönliches Adressbuch, Anrufprotokoll, Telefonmarke, Telefoneinstellungen

Zahlungsinformation

Zahlungsinformation

Mobilfunkanbieter

Besuchte Webseiten, Gesendete Nachrichten, Chatnachrichten, Anrufprotokoll, Gespeicherte Cookies, Persönliche Nachrichten, Kaufverhalten, Beiträge/Postings, Verweildauer, #Hashtags, Likes, Reaktionen (Emojis), Hochgeladene Files/Videos, Interaktio

Kommentare, Telefoneinstellungen

Politische Ansichten, Religiöse Ansichten, Gewerkschaftszugehörigkeit

Gesendete Nachrichten, Chatnachrichten, Anrufprotokoll, Persönliche Nachrichten, Kaufverhalten, Nutzernamen, Kontakte, Freunde, Beiträge/Postings, #Hashtags, Likes, Reaktionen (Emojis), Profil-Foto, Hochgeladene Files/Videos, Follower, Interaktionen, G

Besuchte Webseiten, Geo-Tag, Gesendete Nachrichten, Chatnachrichten, Anrufprotokoll, Gespeicherte Cookies, GPS-Standort, Beiträge/Postings, Verweildauer, #Hashtags, Likes, Reaktionen (Emojis), Hochgeladene Files/Videos, Interaktionen, Markierunge

Kaufverhalten, Interessen, Politische Ansichten

Zahlungsinformation

Nr.	Bezeichnung	Haupt-Cluster
1	Mobilfunkanbieter	Cluster 4
2	Geräte-ID	Cluster 4
3	Name	Cluster 3
4	E-Mailadresse	Cluster 3
5	Wohnort	Cluster 3
6	Alter	Cluster 3
7	Geburtsdatum	Cluster 3
8	Gesichtserkennung	Cluster 2
9	Besuchte Webseiten	Cluster 4
10	Persönliches Adressbuch	Cluster 2
11	Geo-Tag	Cluster 4
12	Zahlungsinformation	Cluster 2
13	Gesendete Nachrichten	Cluster 2
14	Chatnachrichten	Cluster 2
15	Anrufprotokoll	Cluster 2
16	Gespeicherte Cookies	Cluster 4
17	GPS-Standort	Cluster 4
18	Persönliche Nachrichten	Cluster 2
19	Kaufverhalten	Cluster 2
20	Nutzername	Cluster 1
21	Kontakte	Cluster 1
22	Freunde	Cluster 1
23	Beiträge/Postings	Cluster 1
24	Verweildauer	Cluster 1
25	#Hashtags	Cluster 1
26	Likes	Cluster 1
27	Reaktionen (Emojis)	Cluster 1
28	Profil-Foto	Cluster 1
29	Hochgeladene Files/Videos	Cluster 1
30	Follower	Cluster 1
31	Interaktionen	Cluster 1
32	Markierungen (Tags)	Cluster 1
33	Gruppen (öffentlich/privat)	Cluster 1
34	Kommentare	Cluster 1
35	Gesundheitsdaten	Cluster 2
36	Sexuelle Orientierung	Cluster 2
37	Biometrische Daten	Cluster 2
38	Genutzte Geräte	Cluster 4
39	Telefonmarke	Cluster 4
40	TelefonEinstellungen	Cluster 4
41	Verwendetes Betriebssystem	Cluster 4
42	IP-Adresse	Cluster 4
43	Nationalität	Cluster 3
44	Interessen	Cluster 3
45	Geschlecht	Cluster 3
46	Beruf	Cluster 3
47	Politische Ansichten	Cluster 2
48	Religiöse Ansichten	Cluster 2
49	Gewerkschaftszugehörigkeit	Cluster 2
50	Ethnische Herkunft	Cluster 3

Anzahl Cluster 1	15
Anzahl Cluster 2	14
Anzahl Cluster 3	10
Anzahl Cluster 4	11

