

Leitlinien



**Leitlinien 03/2022 zu
irreführenden Gestaltungsmustern auf
Benutzeroberflächen von Social-Media-Plattformen:
wie man sie erkennt und vermeidet**

Version 2.0

Angenommen am 14. Februar 2023

Versionsverlauf

| | | |
|-------------|------------------|-------------------------------------------------------|
| Version 2.0 | 14. Februar 2023 | Annahme der Leitlinien nach öffentlicher Konsultation |
| Version 1.0 | 14. März 2022 | Annahme der Leitlinien zur öffentlichen Konsultation |

ZUSAMMENFASSUNG

Diese Leitlinien enthalten praktische Empfehlungen für Social-Media-Anbieter als Verantwortliche sozialer Medien (nachfolgend auch „Anbieter“) sowie für Designer:innen und Nutzer:innen von Social-Media-Plattformen (nachfolgend auch „Plattformen“) hinsichtlich der Erkennung und Vermeidung irreführender Gestaltungsmuster (sogenannter „Deceptive Design Patterns“) auf Benutzeroberflächen sozialer Medien, die gegen die Anforderungen der DS-GVO verstoßen. Der EDSA empfiehlt, dass die Verantwortlichen zu diesem Zweck interdisziplinäre Teams einsetzen, die unter anderem aus Designer:innen, Datenschutzbeauftragten und Entscheidungsträger:innen bestehen. In diesem Zusammenhang ist zu beachten, dass die Auflistung der irreführenden Gestaltungsmuster und Best Practices sowie der Anwendungsfälle nicht abschließend sind. Social-Media-Anbieter sind für die Datenschutzkonformität ihrer Plattformen weiterhin verantwortlich und rechenschaftspflichtig.

Irreführende Gestaltungsmuster auf Benutzeroberflächen von Social-Media-Plattformen

Im Kontext dieser Leitlinien gelten „irreführende Gestaltungsmuster“ als Benutzeroberflächen und Nutzererfahrungen, die auf Social-Media-Plattformen eingesetzt werden und darauf abzielen, Nutzer:innen dahingehend zu beeinflussen, dass sie unbeabsichtigte, ihnen widerstrebende und potenziell schädliche Entscheidungen treffen, die hinsichtlich der Verarbeitung ihrer personenbezogenen Daten häufig ihren Interessen zuwiderlaufen und die Interessen der Social-Media-Plattformen begünstigen. Irreführende Gestaltungsmuster zielen darauf ab, das Verhalten der Nutzer:innen zu beeinflussen und können deren Fähigkeit beeinträchtigen, ihre personenbezogenen Daten wirksam zu schützen und bewusste Entscheidungen zu treffen. Die Datenschutzbehörden sind dafür verantwortlich, die Verwendung irreführender Gestaltungsmuster zu sanktionieren, wenn diese gegen die Anforderungen der DS-GVO verstoßen. Die in diesen Leitlinien behandelten irreführenden Gestaltungsmuster lassen sich in folgende Kategorien unterteilen:

- **Überfrachtung** bedeutet, dass die Nutzer:innen mit einer Lawine bzw. einer großen Zahl von Anfragen, Informationen, Optionen oder Möglichkeiten konfrontiert werden, damit sie veranlasst werden, mehr Daten preiszugeben oder entgegen den Erwartungen der betroffenen Person unbeabsichtigt die Verarbeitung personenbezogener Daten zuzulassen. In diese Kategorie fallen die drei folgenden Arten irreführender Gestaltungsmuster: ***Ständige Aufforderungen, Datenschutz-Labyrinth*** und ***Zu viele Optionen***
- **Überspringen** bedeutet, die Benutzeroberfläche oder Nutzererfahrung so zu gestalten, dass die Nutzer:innen alle oder einige Datenschutzaspekte vergessen oder nicht bedenken. In diese Kategorie fallen die beiden folgenden Arten irreführender Gestaltungsmuster: ***Trügerische Bequemlichkeit*** und ***Schau, dort drüben***
- **Aufwühlen** wirkt sich mittels Ansprechen von Emotionen oder visueller „Anreize“ auf die Wahl aus, die Nutzer:innen treffen. In diese Kategorie fallen die beiden folgenden Arten irreführender Gestaltungsmuster: ***Emotionale Steuerung*** und ***Vor aller Augen verborgen***

- **Behindern** bedeutet, Nutzer:innen daran zu hindern oder ihnen den Weg zu versperren, sich zu informieren oder ihre Daten zu verwalten, indem die jeweilige Handlung erschwert oder unmöglich gemacht wird.
In diese Kategorie fallen die drei folgenden Arten irreführender Gestaltungsmuster: ***Sackgasse, Länger als erforderlich*** und ***Irreführende Handlung***
- **Unbeständig** bedeutet, dass die Gestaltung der Benutzeroberfläche uneinheitlich und unklar ist, wodurch es Nutzer:innen erschwert wird, die verschiedenen Instrumente zur Kontrolle der Datenschutzeinstellungen zu steuern und den Zweck der Verarbeitung nachzuvollziehen.
In diese Kategorie fallen die folgenden vier Kategorien irreführender Gestaltungsmuster: ***Fehlende Hierarchie, Dekontextualisierung, Uneinheitliche Benutzeroberfläche*** und ***Sprachliche Diskontinuität***
- **Im Dunkeln gelassen** bedeutet, dass eine Benutzeroberfläche so konzipiert ist, dass Informationen oder Instrumente zur Kontrolle der Datenschutzeinstellungen verborgen werden oder Nutzer:innen im Ungewissen gelassen werden, wie ihre Daten verarbeitet werden und welche Art von Kontrolle sie in Bezug auf die Ausübung ihrer Rechte haben können.
In diese Kategorie fallen die beiden folgenden Arten irreführender Gestaltungsmuster: ***Widersprüchliche Informationen*** und ***Mehrdeutige Formulierungen oder Informationen***

Maßgebliche Rechtsvorschriften der DS-GVO zur Bewertung irreführender Gestaltungsmuster

Was die Einhaltung des Datenschutzes durch Benutzeroberflächen von Online-Anwendungen innerhalb des Sektors der sozialen Medien betrifft, so sind die geltenden Datenschutzgrundsätze in Artikel 5 DS-GVO festgelegt. Der in Artikel 5 Absatz 1 Buchstabe a DS-GVO verankerte Grundsatz der Verarbeitung nach Treu und Glauben dient als Ausgangspunkt für die Beurteilung, ob ein Gestaltungsmuster tatsächlich ein „irreführendes Gestaltungsmuster“ darstellt. Weitere Grundsätze, die bei dieser Bewertung eine Rolle spielen, sind die Grundsätze der Transparenz, der Datenminimierung und der Rechenschaftspflicht nach Artikel 5 Absatz 1 Buchstaben a und c und Absatz 2 DS-GVO sowie in manchen Fällen die Zweckbindung gemäß Artikel 5 Absatz 1 Buchstabe b DS-GVO. In anderen Fällen stützt sich die rechtliche Beurteilung auch auf die Bedingungen der Einwilligung nach Artikel 4 Nummer 11 und Artikel 7 DS-GVO oder auf andere spezifische Verpflichtungen wie Artikel 12 DS-GVO. Es liegt auf der Hand, dass im Zusammenhang mit den Rechten betroffener Personen auch das dritte Kapitel der DS-GVO zu berücksichtigen ist. Schließlich spielen die Anforderungen des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen aus Artikel 25 DS-GVO eine entscheidende Rolle, da ihre Anwendung vor der Einführung eines Benutzeroberflächen-Designs die Anbieter darin unterstützen würde, irreführende Gestaltungsmuster von vornherein zu vermeiden.

Beispiele für irreführende Gestaltungsmuster in Anwendungsfällen des Lebenszyklus eines Kontos in sozialen Medien

Die Bestimmungen der DS-GVO gelten für den gesamten Verlauf der Verarbeitung personenbezogener Daten im Rahmen des Betriebs von Social-Media-Plattformen, d. h. für den gesamten Lebenszyklus eines Nutzerkontos. Der EDSA benennt konkrete Beispiele für Kategorien irreführender Gestaltungsmuster im Hinblick auf die folgenden unterschiedlichen Anwendungsfälle innerhalb dieses

Lebenszyklus: die Anmeldung, d. h. das Registrierungsverfahren; Anwendungsfälle in Bezug auf Informationen in den Datenschutzhinweisen, die gemeinsame Verantwortlichkeit und die Kommunikation über Verletzungen des Schutzes personenbezogener Daten; die Einwilligung und das Datenschutzmanagement; die Ausübung der Rechte betroffener Personen bei der Nutzung sozialer Medien; und schließlich die Schließung eines Kontos in sozialen Medien. Verbindungen zu den Bestimmungen der DS-GVO werden auf zweierlei Weise erläutert: Erstens wird bei jedem Anwendungsfall ausführlicher erläutert, welche der oben genannten DS-GVO-Bestimmungen für den betreffenden Fall besonders relevant sind. Zweitens wird in den Randnummern rund um die Beispiele für irreführende Gestaltungsmuster erläutert, in welcher Weise sie gegen die DS-GVO verstoßen.

Empfehlungen für Best Practices

Neben den Beispielen für irreführende Gestaltungsmuster werden in den Leitlinien am Ende jedes Anwendungsfalls sowie in Anhang II auch Best Practices dargestellt. Diese enthalten spezifische Empfehlungen für die Gestaltung von Benutzeroberflächen, die die wirksame Umsetzung der DS-GVO erleichtern.

Checkliste für irreführende Gestaltungsmuster

Eine Checkliste für irreführende Gestaltungsmuster ist in Anhang I dieser Leitlinien zu finden. Der Anhang bietet einen Überblick über die oben aufgeführten Kategorien und Arten irreführender Gestaltungsmuster sowie eine Liste von Beispielen für die einzelnen, in den Anwendungsfällen genannten, Muster. Für manche Leser kann es hilfreich sein, die Checkliste als Ausgangspunkt zu nutzen, um sich mit diesen Leitlinien vertraut zu machen.

Inhaltsverzeichnis

| | | |
|-------|------------------------------------------------------------------------------------------------------------------------------------|----|
| 1 | Anwendungsbereich | 8 |
| 2 | Anwendbare Grundsätze – Was ist zu beachten? | 12 |
| 2.1 | Rechenschaftspflicht | 13 |
| 2.2 | Transparenz..... | 13 |
| 2.3 | Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen..... | 14 |
| 3 | Lebenszyklus eines Nutzerkontos in sozialen Medien: praktische Umsetzung der Grundsätze ... | 16 |
| 3.1 | Eröffnung eines Nutzerkontos | 16 |
| | Anwendungsfall 1: Registrierung eines Nutzerkontos..... | 16 |
| 3.2 | In den sozialen Medien auf dem Laufenden bleiben..... | 30 |
| | Anwendungsfall 2a: Mehrschichtige Datenschutzhinweise | 30 |
| | Anwendungsfall 2b: Unterrichtung der betroffenen Person über gemeinsame Verantwortlichkeit, Artikel 26 Absatz 2 DS-GVO | 37 |
| | Anwendungsfall 2c: Benachrichtigung der betroffenen Person im Falle einer Verletzung des Schutzes personenbezogener Daten | 38 |
| 3.3 | In den sozialen Medien geschützt bleiben..... | 42 |
| | Anwendungsfall 3a: Verwalten der Einwilligung während der Nutzung einer Social-Media- Plattform | 42 |
| | Anwendungsfall 3b: Verwalten der Datenschutzeinstellungen | 51 |
| 3.4 | Richtig unterwegs in den sozialen Medien: Rechte betroffener Personen | 59 |
| | Anwendungsfall 4: Wie man angemessene Anwendungen für die Ausübung der Rechte betroffener Personen bereitstellt | 59 |
| 3.5 | Tschüss und Auf Wiedersehen: Ein Nutzerkonto in sozialen Medien verlassen | 70 |
| | Anwendungsfall 5: Vorübergehendes Pausieren des Kontos/Löschung aller personenbezogenen Daten | 70 |
| 4 | Anhang I: Verzeichnis der Kategorien und Arten irreführender Gestaltungsmuster | 79 |
| 4.1 | Überfrachtung | 79 |
| 4.1.1 | Ständige Aufforderungen | 79 |
| 4.1.2 | Datenschutz-Labyrinth | 80 |
| 4.1.3 | Zu viele Optionen | 80 |
| 4.2 | Überspringen..... | 80 |
| 4.2.1 | Trügerische Bequemlichkeit | 80 |
| 4.2.2 | „Schau, dort drüben“..... | 81 |
| 4.3 | Aufwühlen | 81 |
| 4.3.1 | Emotionale Steuerung..... | 81 |
| 4.3.2 | Vor aller Augen verborgen | 82 |

| | | |
|-------|----------------------------------------------------|----|
| 4.4 | Behindern | 82 |
| 4.4.1 | Sackgasse..... | 82 |
| 4.4.2 | Länger als erforderlich..... | 83 |
| 4.4.3 | Irreführende Handlungen..... | 83 |
| 4.5 | Unbeständig | 83 |
| 4.5.1 | Fehlende Hierarchie | 83 |
| 4.5.2 | Dekontextualisierung..... | 84 |
| 4.5.3 | Uneinheitliche Benutzeroberfläche..... | 84 |
| 4.5.4 | Sprachliche Diskontinuität..... | 84 |
| 4.6 | Im Dunkeln gelassen..... | 85 |
| 4.6.1 | Widersprüchliche Informationen | 85 |
| 4.6.2 | Mehrdeutige Formulierungen oder Informationen..... | 85 |
| 5 | Anhang II: Best Practices | 88 |

Der Europäische Datenschutzausschuss —

gestützt auf Artikel 70 Absatz 1 Buchstabe e der 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, im Folgenden „DS-GVO“),

gestützt auf das EWR-Abkommen, insbesondere auf Anhang XI und das Protokoll 37, in der durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018 geänderten Fassung,¹

gestützt auf Artikel 12 und Artikel 22 seiner Geschäftsordnung —

HAT DIE FOLGENDEN LEITLINIEN ANGENOMMEN

1 ANWENDUNGSBEREICH

1. Ziel dieser Leitlinien ist es, Empfehlungen und Orientierungshilfen für die Gestaltung der Benutzeroberflächen von Social-Media-Plattformen zu geben. Für die Zwecke dieser Leitlinien bezeichnen soziale Medien Online-Plattformen, die die Entwicklung von Netzwerken und Gemeinschaften von Nutzer:innen ermöglichen, in denen Informationen und Inhalte geteilt werden.² Die Leitlinien können entweder in der Konzeptionsphase einer Benutzeroberfläche verwendet werden, um die Implementierung irreführender Gestaltungsmuster³ von Anfang an zu vermeiden, oder zur Bewertung der Konformität der Benutzeroberfläche bei einem bestehenden Dienst. Sie richten sich an Social-Media-Anbieter als Verantwortliche für die Gestaltung und den Betrieb von Social-Media-Plattformen. In diesem Zusammenhang besteht das Ziel der Leitlinien darin, auf die Verpflichtungen hinzuweisen, die sich aus der DS-GVO ergeben, insbesondere in Bezug auf die Grundsätze der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung und Datenminimierung bei der Gestaltung von Benutzeroberflächen und der Darstellung von Inhalten ihrer Webdienste und Apps. Die genannten Grundsätze müssen im Wesentlichen umgesetzt werden und stellen aus technischer Sicht Anforderungen an die Gestaltung von Software und Diensten dar, einschließlich Benutzeroberflächen. Es wird eine eingehende Untersuchung zu den Anforderungen der DS-GVO hinsichtlich ihrer Anwendung auf Benutzeroberflächen und die Darstellung von Inhalten durchgeführt; in diesem Rahmen wird erläutert, was als „irreführendes Gestaltungsmuster“ gilt, d. h. als Methode der Gestaltung und Darstellung von Inhalten, die erheblich gegen diese Anforderungen verstößt, bei der aber der Anschein erweckt wird, dass sie formell den Anforderungen entspricht. Diese Leitlinien sind auch geeignet, das Bewusstsein der Nutzer:innen für ihre Rechte und für die Risiken zu schärfen, die sich aus der Weitergabe zu vieler Daten oder einer unkontrollierten Weitergabe ihrer

¹ Soweit in diesem Dokument auf „Mitgliedstaaten“ Bezug genommen wird, ist dies als Bezugnahme auf „EWR-Mitgliedstaaten“ zu verstehen.

² Die Definition ist identisch mit der in den EDSA-Leitlinien 8/2020 über die gezielte Ansprache von Nutzer:innen sozialer Medien, Rn. 1; eine ausführlichere Beschreibung ist der Fußnote 1 dort zu entnehmen; abrufbar unter https://edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_de_0.pdf.

³ Für Version 2.0 dieser Leitlinien verwendet der EDSA statt „Dark Pattern“ den umfassenderen und stärker beschreibenden Begriff „irreführendes Gestaltungsmuster“.

Daten ergeben könnten. Ein weiteres Ziel dieser Leitlinien besteht darin, Nutzer:innen darin zu schulen, wie man „irreführende Gestaltungsmuster“ (gemäß der nachfolgenden Definition) erkennt und ihnen begegnet, um die eigene Privatsphäre bewusst zu schützen. Im Rahmen der Auswertung wurde der Lebenszyklus eines Kontos in sozialen Medien anhand von fünf Anwendungsfällen untersucht: „Eröffnung eines Nutzerkontos“ (Anwendungsfall 1), „In den sozialen Medien auf dem Laufenden bleiben“ (Anwendungsfall 2), „In den sozialen Medien geschützt bleiben“ (Anwendungsfall 3), „Richtig unterwegs in den sozialen Medien: Rechte betroffener Personen“ (Anwendungsfall 4) und „Tschüss und Auf Wiedersehen: Ein Nutzerkonto in sozialen Medien verlassen“ (Anwendungsfall 5).

2. In diesen Leitlinien bezieht sich der Begriff „Benutzeroberfläche“ auf das Instrument, das Menschen für die Interaktion mit Social-Media-Plattformen nutzen können. Der Schwerpunkt des Dokuments liegt auf grafischen Benutzeroberflächen (z. B. für Computer- und Smartphone-Benutzeroberflächen), einige der Beobachtungen können jedoch auch für sprachgesteuerte Benutzeroberflächen (z. B. für intelligente Lautsprecher) oder gestenbasierte Benutzeroberflächen (z. B. in virtueller Realität) gelten. Der Begriff „Nutzererlebnis“ bezeichnet die verschiedenen Handlungen oder Schritte, die die Nutzer:innen durchführen, um ihr Ziel zu erreichen; in sozialen Netzwerken kann es sich dabei um das Durchsuchen von Feeds, das Teilen eines Posts, die Festlegung von Präferenzen usw. handeln. Der Begriff „Nutzererfahrung“ bezeichnet die allgemeinen Erfahrungen, die Nutzer:innen mit Social-Media-Plattformen haben; hierzu zählen der wahrgenommene Nutzen, die Benutzerfreundlichkeit und die Effizienz der Interaktion mit der Plattform. Die Gestaltung der Benutzeroberflächen und die Gestaltung des Nutzererlebnisses haben sich in den letzten zehn Jahren kontinuierlich weiterentwickelt. In jüngster Zeit setzten sich zunehmend flächendeckende, maßgeschneiderte, als nahtlos bezeichnete Nutzerinteraktionen und -erlebnisse durch: Die perfekte Benutzeroberfläche sollte in hohem Maße personalisiert, benutzerfreundlich und multimodal sein.⁴ Auch wenn diese Trends vielleicht die Benutzerfreundlichkeit der Nutzung digitaler Dienste erhöhen, können sie doch in einer Weise genutzt werden, um in erster Linie Nutzerverhalten zu fördern, das dem Geist der DS-GVO zuwiderläuft.⁵ Dies ist insbesondere im Kontext der Aufmerksamkeitsökonomie von Bedeutung, in der die Aufmerksamkeit der Nutzer:innen als Ware gilt. In diesen Fällen können die rechtlich zulässigen Grenzen der DS-GVO überschritten werden; die Gestaltung von Benutzeroberflächen und die Gestaltung von Nutzerlebenissen, die Fälle dieser Art nach sich ziehen, werden nachstehend als „irreführende Gestaltungsmuster“ beschrieben.
3. Im Kontext dieser Leitlinien gelten „irreführende Gestaltungsmuster“ als Benutzeroberflächen und Nutzererlebnisse, die auf Social-Media-Plattformen eingesetzt werden und darauf abzielen, Nutzer:innen dahingehend zu beeinflussen, dass sie unbeabsichtigte, ihnen widerstrebende und potenziell schädliche Entscheidungen treffen, die hinsichtlich der Verarbeitung ihrer personenbezogenen Daten häufig ihren Interessen zuwiderlaufen und die Interessen der Plattformen begünstigen. Irreführende Gestaltungsmuster zielen darauf ab, das Verhalten der Nutzer:innen zu beeinflussen, das sich im Allgemeinen auf kognitive Voreingenommenheiten stützt; sie können die Fähigkeit der Nutzer:innen beeinträchtigen, „ihre personenbezogenen Daten wirksam zu schützen und bewusste Entscheidungen zu treffen“,⁶ indem sie es ihnen unmöglich machen, „eine

⁴ Für weitere Einzelheiten siehe CNIL, IP Report No. 6: Shaping Choices in the Digital World, 2019. S. 9 https://www.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf.

⁵ CNIL, Shaping Choices in the Digital World, 2019. S. 10.

⁶ CNIL, Shaping Choices in the Digital World, 2019. S. 27.

in informierter Weise und freiwillig erteilte Einwilligung zu geben“⁷. Dies kann bei mehreren Aspekten der Gestaltung genutzt werden, z. B. bei der Farbwahl der Benutzeroberflächen und der Anordnung des Inhalts. Umgekehrt kann die Umsetzung von Datenschutzvorschriften durch Anreize und nutzerfreundliche Gestaltungen gefördert werden.

4. Irreführende Gestaltungsmuster führen nicht unbedingt nur zu einem Verstoß gegen Datenschutzvorschriften. Irreführende Gestaltungsmuster können beispielsweise auch Verbraucherschutzvorschriften verletzen. Die Grenzen zwischen Verstößen, die von Datenschutzbehörden durchgesetzt werden können, und solchen, die durch nationale Verbraucherschutz-, Wettbewerbs- oder andere Behörden durchsetzbar sind, können fließend sein.⁸ Gemäß der DS-GVO sind die Datenschutzbehörden dafür zuständig, die Verwendung irreführender Gestaltungsmuster zu sanktionieren, wenn diese tatsächlich gegen Datenschutzstandards und somit gegen die DS-GVO verstoßen. Verstöße gegen die Anforderungen der DS-GVO müssen einer Einzelfallprüfung unterzogen werden. In diesen Leitlinien werden nur irreführende Gestaltungsmuster behandelt, die unter diese aufsichtsrechtliche Aufgabe fallen könnten. Aus diesem Grund werden in den Leitlinien neben Beispielen irreführender Gestaltungsmuster auch Best Practices dargestellt, die für die Konzipierung von Benutzeroberflächen eingesetzt werden können, mit denen die wirksame Umsetzung der DS-GVO erleichtert wird. Solche Best Practices können einen ersten Schritt auf dem Weg zu einer standardisierten Methode darstellen, mit der Nutzer:innen ihre Daten wirksam kontrollieren und ihre Rechte ausüben können.
5. Die in diesen Leitlinien behandelten irreführenden Gestaltungsmuster⁹ sind das Ergebnis einer interdisziplinären Analyse bestehender Benutzeroberflächen und lassen sich in folgende Kategorien einteilen:

Überfrachtung: die Nutzer:innen werden mit einer Lawine bzw. einer großen Zahl von Anfragen, Informationen, Optionen oder Möglichkeiten konfrontiert, um sie zu veranlassen, mehr Daten preiszugeben oder entgegen den Erwartungen der betroffenen Person die Verarbeitung personenbezogener Daten zuzulassen.

Überspringen: Gestaltung der Schnittstelle oder Nutzerreise in einer Weise, dass die Nutzer:innen alle oder einige Datenschutzaspekte vergessen oder nicht bedenken.

Aufwühlen: wirkt sich mittels Ansprechen von Emotionen oder visueller „Anreize“ auf die Wahl aus, die Nutzer:innen treffen.

⁷ Siehe Norwegischer Verbraucherrat, *Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy*, S. 10 <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>, aber auch CNIL, *Shaping Choices in the Digital World*, S. 30-31.

⁸ In diesem Zusammenhang wird in Artikel 25 Absatz 2 der Verordnung (EU) 2022/2065 vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste) klargestellt, dass das in Artikel 25 Absatz 1 enthaltene Verbot, Online-Schnittstellen so zu konzipieren, dass Nutzer getäuscht oder manipuliert werden, nicht für Praktiken gilt, die unter die Richtlinie 2005/29/EG (Richtlinie über unlautere Geschäftspraktiken im Geschäftsverkehr zwischen Unternehmen und Verbrauchern, UGPRL) oder die DS-GVO fallen. Darüber hinaus enthält die Bekanntmachung der EU-Kommission (2021/C 526/01) Leitlinien zur Auslegung und Anwendung der UGPRL, einschließlich zu „Dark Patterns“ in Abschnitt 4.2.7.

⁹ Kategorien irreführender Gestaltungsmuster und Arten irreführender Gestaltungsmuster innerhalb dieser Kategorien werden im Text der Leitlinien **fett und kursiv** gedruckt dargestellt. Der Anhang enthält eine ausführliche Übersicht.

Behindern: Nutzer:innen werden daran gehindert oder es wird ihnen der Weg versperrt, sich zu informieren oder ihre Daten zu verwalten, indem die jeweilige Handlung erschwert oder unmöglich gemacht wird.

Unbeständig: die Gestaltung der Schnittstelle ist uneinheitlich und unklar, wodurch es für Nutzer:innen schwierig wird, die verschiedenen Instrumente zur Datenschutzkontrolle zu navigieren und den Zweck der Verarbeitung zu verstehen.

Im Dunkeln gelassen: eine Schnittstelle ist so konzipiert, dass Informationen oder Instrumente der Datenschutzkontrolle verborgen werden oder Nutzer:innen im Ungewissen gelassen werden, wie ihre Daten verarbeitet werden und welche Art von Kontrolle sie in Bezug auf die Ausübung ihrer Rechte haben könnten.

6. Neben der Eingruppierung irreführender Gestaltungsmuster in diese Kategorien anhand ihrer Auswirkungen auf das Nutzerverhalten können diese Muster auch in inhalts- und oberflächenbezogene Muster unterteilt werden, wodurch Aspekte der Benutzeroberfläche oder der Nutzererlebnisse ausführlicher behandelt werden können. Inhaltsbezogene Muster beziehen sich auf den tatsächlichen Inhalt und damit auch auf den Wortlaut und Kontext der Sätze und Informationsbestandteile. Darüber hinaus gibt es jedoch auch Komponenten, die sich unmittelbar auf die Wahrnehmung dieser Faktoren auswirken. Diese oberflächenbezogenen Muster beziehen sich auf die Art und Weise, wie der Inhalt angezeigt wird, wie man durch ihn navigiert oder mit ihm interagiert wird.
7. Unbedingt zu berücksichtigen ist, dass irreführende Gestaltungsmuster zusätzliche Bedenken aufwerfen hinsichtlich möglicher Auswirkungen auf Kinder¹⁰, die sich bei Social-Media-Plattformen anmelden, sowie auf andere schutzbedürftige Gruppen wie ältere Menschen, sehbehinderte Menschen oder Menschen, die digital weniger erfahren sind als andere. Schutzbedürftige Gruppen wie ältere Nutzer:innen sind häufig nicht nur weniger gut in der Lage, manipulative Gestaltungspraktiken zu erkennen, sondern ihnen ist auch weniger bewusst, dass ihr digitales Verhalten Beeinflussungen unterliegt. Für den Fall, dass die Verarbeitung personenbezogener Daten von Kindern betrifft, schreibt die DS-GVO zusätzliche Schutzmaßnahmen vor, da Letztere sich der betreffenden Risiken und Folgen und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind.¹¹ In Erwägungsgrund 58 wird ausdrücklich darauf hingewiesen, dass dann, wenn sich die Verarbeitung an Kinder richtet, Informationen in einer klaren und einfachen Sprache erfolgen sollten, sodass Kinder sie verstehen können. Darüber hinaus schließt die DS-GVO ausdrücklich die Verarbeitung von Daten natürlicher Personen, insbesondere von Kindern, in die Situationen ein, in denen die Risiken für die Rechte und Freiheiten von Personen – mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere – aus einer Datenverarbeitung hervorgehen können, die zu einem physischen, materiellen oder immateriellen Schaden führen können.¹²
8. In Anbetracht dessen sollte man sich darüber im Klaren sein, dass irreführende Gestaltungsmuster nicht nur auf Social-Media-Plattformen beschränkt sind. In der öffentlichen Konsultation zu diesen Leitlinien wurden deutliche Meinungen zu diesem Thema geäußert. Auch in vielen anderen Fällen, in denen auf der Basis von oder im Zusammenhang mit Datenverarbeitungsvorgängen Interaktionen zwischen Nutzer:innen und Produkten sowie Diensten stattfinden, gibt es Benutzeroberflächen. Hierzu

¹⁰ Siehe auch Erwägungsgrund 81 Satz 4 der Verordnung (EU) 2022/2065 (Gesetz über digitale Dienste).

¹¹ DS-GVO, Erwägungsgrund 38.

¹² DS-GVO, Erwägungsgrund 75; siehe auch EDSA-Leitlinien 8/2020 über die gezielte Ansprache von Nutzer:innen sozialer Medien, Rn. 16 https://edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_de_0.pdf.

können Websites und Cookie-Banner¹³, Videospiele, mobile Anwendungen, Kleinbetragszahlungen usw. zählen. Obwohl die nachstehend beschriebenen irreführenden Gestaltungsmuster möglicherweise nicht in genau derselben, hier beschriebenen Form vorliegen, können sie dennoch die Rechte der betroffenen Personen oder der Verbraucher verletzen. Der Schwerpunkt dieser Leitlinien liegt jedoch ausschließlich auf irreführenden Gestaltungsmustern auf Social-Media-Plattformen, da der Einfluss dieser Plattformen auf das tägliche Leben von Menschen und Nationen stetig zunimmt, wie in früheren Dokumenten des EDSA verdeutlicht wurde.¹⁴

2 ANWENDBARE GRUNDSÄTZE – WAS IST ZU BEACHTEN?

9. Was die Einhaltung des Datenschutzes durch Benutzeroberflächen von Online-Anwendungen im Bereich der sozialen Medien betrifft, so sind die geltenden Datenschutzgrundsätze in Artikel 5 DS-GVO festgelegt. Der in Artikel 5 Absatz 1 Buchstabe a DS-GVO verankerte Grundsatz der Verarbeitung nach Treu und Glauben ist ein Ausgangspunkt für die Bewertung des Vorliegens irreführender Gestaltungsmuster. Wie der EDSA bereits feststellte, ist die Verarbeitung nach Treu und Glauben ein übergeordneter Grundsatz, nach dem personenbezogene Daten nicht auf eine Weise verarbeitet werden dürfen, die für die betroffene Person in nicht gerechtfertigter Weise schädlich, widerrechtlich diskriminierend, unerwartet oder irreführend ist.¹⁵ Sind in der Benutzeroberfläche unzureichende oder irreführende Informationen für die Nutzer:innen vorhanden und erfüllt sie die Merkmale irreführender Gestaltungsmuster, kann sie als gegen Treu und Glauben verstoßende Verarbeitung eingestuft werden. Der Grundsatz der Verarbeitung nach Treu und Glauben hat eine übergreifende Funktion und alle irreführenden Gestaltungsmuster wären – unabhängig von der Einhaltung anderer Datenschutzgrundsätze – mit diesem Grundsatz nicht vereinbar.
10. Neben dieser grundlegenden Vorschrift der Verarbeitung nach Treu und Glauben sind auch die Grundsätze der Rechenschaftspflicht, der Transparenz und der Verpflichtung zum Datenschutz durch Technikgestaltung gemäß Artikel 25 DS-GVO im Hinblick auf den Gestaltungsrahmen relevant, und irreführende Gestaltungsmuster könnten gegen diese Bestimmungen verstoßen. Es ist jedoch auch möglich, dass die rechtliche Bewertung irreführender Gestaltungsmuster auf Elementen beruht, die sich auf allgemeine Begriffsbestimmungen wie in Artikel 4 Nummer 11 DS-GVO, die Definition des Begriffs „Einwilligung“ oder andere spezifische Verpflichtungen wie in Artikel 12 DS-GVO stützen. Nach Artikel 12 Absatz 1 Satz 1 DS-GVO sind die Verantwortlichen verpflichtet, geeignete Maßnahmen zu treffen, um alle Mitteilungen im Zusammenhang mit den Rechten betroffener Personen sowie alle Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren

¹³ Aufgrund einer Reihe von Beschwerden, die vom Europäischen Zentrum für digitale Rechte NOYB übermittelt wurden, führte eine EDSA-Taskforce einen Meinungsaustausch über eine Reihe von Gestaltungselementen in Cookie-Bannern durch. Der gemeinsame Nenner, auf den sich die Aufsichtsbehörden bei ihrer Auslegung des geltenden, mehrere Ebenen umfassenden Rechtsrahmens einigten, wurde in einem Bericht über die Arbeit der Cookie-Banner-Taskforce vom 17. Januar 2023 zusammengefasst, der unter https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf abrufbar ist.

¹⁴ EDSA-Leitlinien 8/2020 für die gezielte Ansprache von Nutzer:innen sozialer Medien, Erklärung Nr. 2/2019 zur Verwendung personenbezogener Daten im Rahmen politischer Kampagnen https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-22019-use-personal-data-course-political_de.

¹⁵ EDSA-Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Version 2.0, angenommen am 20. Oktober 2020, S. 16; https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_de.

und einfachen Sprache zu übermitteln. Wie aus Erwägungsgrund 39 Satz 3 zum Grundsatz der Transparenz hervorgeht, ist dieses Erfordernis jedoch nicht auf Datenschutzhinweise¹⁶ oder Rechte betroffener Personen¹⁷ beschränkt, sondern gilt für alle Informationen und Mitteilungen zur Verarbeitung personenbezogener Daten. In Satz 5 des Erwägungsgrundes wird auch klargestellt, dass die betroffenen Personen über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten informiert und darüber aufgeklärt werden sollten, wie sie ihre diesbezüglichen Rechte geltend machen können.

11. Wichtig bei der Gestaltung von Benutzeroberflächen von Online-Anwendungen ist auch die Berücksichtigung des Grundsatzes der Zweckbindung nach Artikel 5 Absatz 1 Buchstabe b DS-GVO sowie des Grundsatzes der Datenminimierung nach Artikel 5 Absatz 1 Buchstabe c der DS-GVO. Die Verantwortlichen sind in jedem Fall gut beraten, zur Gewährleistung der Datenschutzkonformität die Einhaltung aller Datenschutzgrundsätze der DS-GVO sehr genau nachzuprüfen.

2.1 Rechenschaftspflicht

12. Der Grundsatz der Rechenschaftspflicht muss sich in der Gestaltung von Benutzeroberflächen stets widerspiegeln.
13. In Artikel 5 Absatz 2 der DS-GVO wird bestimmt, dass ein Verantwortlicher für die Einhaltung der in Artikel 5 Absatz 1 der DS-GVO beschriebenen Grundsätze der DS-GVO verantwortlich ist und deren Einhaltung nachweisen können muss. Dieser Grundsatz steht daher in engem Zusammenhang mit den vorstehend genannten einschlägigen Grundsätzen. Die Rechenschaftspflicht kann durch Elemente gewährleistet werden, die belegen, dass der Social-Media-Anbieter die DS-GVO einhält. Benutzeroberfläche und Nutzererlebnis können als Dokumentationsinstrument genutzt werden, um nachzuweisen, dass die Nutzer:innen während ihrer Aktivitäten auf der Social-Media-Plattform Datenschutzinformationen gelesen und berücksichtigt, ihre Einwilligung freiwillig gegeben, ihre Rechte ohne Schwierigkeiten ausgeübt haben usw. Methoden der qualitativen und quantitativen Nutzerforschung wie A/B-Tests, Eye-Tracking (Blickverfolgung) oder Nutzerinterviews, ihre Ergebnisse und ihre Analyse können ebenfalls zur Unterstützung des Nachweises der Einhaltung der Vorschriften verwendet werden. Hierbei ist zu beachten, dass solche Forschungsmethoden häufig auch die Verarbeitung personenbezogener Daten beinhalten, die daher im Einklang mit der DS-GVO stehen muss. Wenn beispielsweise Nutzer:innen ein Kästchen ankreuzen oder eine von mehreren Datenschutzoptionen anklicken müssen, können Screenshots der Benutzeroberfläche dazu dienen, den Weg der Nutzer:innen durch die Datenschutzinformationen zu zeigen und zu erläutern, wie die Nutzer:innen eine Entscheidung in informierter Weise treffen. Die Ergebnisse der auf der betreffenden Benutzeroberfläche durchgeführten Nutzerforschung können zusätzliche Elemente liefern, aus denen im Einzelnen hervorgeht, warum die Benutzeroberfläche zur Erreichung eines Informationsziels optimal ist.
14. Auf dem Gebiet der Benutzeroberflächen finden sich solche dokumentarischen Elemente in der Offenlegung bestimmter Vereinbarungen, vor allem dann, wenn Beweise, z. B. eine Einwilligung oder eine Lesebestätigung, eingeholt werden.

2.2 Transparenz

15. Der Grundsatz der Transparenz in Artikel 5 Absatz 1 Buchstabe a DS-GVO überschneidet sich stark mit dem Bereich der allgemeinen Rechenschaftspflicht. Auch wenn die Verantwortlichen bestimmte sensible Geschäftsinformationen gegenüber Dritten schützen müssen, könnte es zur Gewährleistung

¹⁶ Behandelt in Teil 3.2. – Anwendungsfall 2a dieser Leitlinien.

¹⁷ Behandelt in den Anwendungsfällen 4 und 5, d. h. Teil 3.4 und 3.5 dieser Leitlinien.

der Rechenschaftspflicht beitragen, die Dokumentation der Verarbeitung zugänglich oder aufzeichnenbar zu gestalten: Eine Lesebestätigung kann beispielsweise für einen Text eingeholt werden, den der Verantwortliche nach dem Grundsatz der Transparenz zur Verfügung stellen muss. Dies kann stets dazu dienen, zugleich auch die Transparenz gegenüber den betroffenen Personen zu gewährleisten.

16. Alle in Artikel 5 der DS-GVO dargelegten Datenschutzgrundsätze werden in der DS-GVO näher erläutert. In Artikel 5 Absatz 1 Buchstabe a DS-GVO ist festgelegt, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden müssen. In den Leitlinien für Transparenz werden die in Artikel 12 DS-GVO festgelegten Elemente der Transparenz im Einzelnen genannt, d. h. die Notwendigkeit, die Informationen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln“.¹⁸ Diese Leitlinien enthalten auch Orientierungshilfen für die Erfüllung der Informationspflichten nach den Artikeln 13 und 14 DS-GVO in Bezug auf Social-Media-Anbieter.
17. Darüber hinaus enthält der Wortlaut der Datenschutzgrundsätze des Artikels 5 Absatz 1 Buchstabe a DS-GVO und anderer besonderer Rechtsvorschriften in der Verordnung zahlreiche weitere Einzelheiten des Transparenzgrundsatzes, die mit spezifischen Rechtsgrundsätzen wie den besonderen Transparenzanforderungen in Artikel 7 DS-GVO für die Einholung der Einwilligung verknüpft sind.

2.3 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

18. In Artikel 25 Absatz 1 DS-GVO wird festgelegt, dass die Verantwortlichen geeignete technische und organisatorische Maßnahmen treffen müssen, die dafür ausgelegt sind, die Datenschutzgrundsätze umzusetzen, während in Artikel 25 Absatz 2 DS-GVO klargestellt wird, dass solche Maßnahmen auch umgesetzt werden müssen, um sicherzustellen, dass durch Voreinstellungen grundsätzlich nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Im Zusammenhang mit den Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen gibt es eine Reihe von Schlüsselementen, die Verantwortliche und Auftragsverarbeiter bei der Umsetzung des Datenschutzes durch Technikgestaltung in Bezug auf eine Social-Media-Plattform berücksichtigen müssen. Eines dieser Elemente besteht darin, dass im Hinblick auf den Grundsatz der Verarbeitung nach Treu und Glauben Informationen über die Datenverarbeitung und Optionen zur Datenverarbeitung objektiv und neutral bereitgestellt werden sollten, wobei weder die Formulierungen noch die Gestaltung irreführend oder manipulativ sein sollten.¹⁹ In den Leitlinien werden Elemente der Grundsätze des Datenschutzes durch datenschutzfreundliche Voreinstellungen und durch Technikgestaltung genannt, die im Hinblick auf irreführende Gestaltungsmuster sogar noch mehr Bedeutung erlangen:²⁰
 - Autonomie – Den betroffenen Personen sollte bei der Bestimmung über die Nutzung ihrer personenbezogenen Daten sowie über Umfang und Bedingungen dieser Nutzung oder Verarbeitung der höchstmögliche Grad an Autonomie gewährt werden.

¹⁸ Artikel-29-Datenschutzgruppe, Guidelines on transparency under Regulation 2016/679, die vom EDSA gebilligt wurden https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

¹⁹ Siehe die Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, S. 21, Rn. 70.

²⁰ Auszug – die vollständige Liste findet sich in den Leitlinien zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Rn. 70.

- Interaktion – Die betroffenen Personen müssen in der Lage sein, ihre Rechte in Bezug auf die von dem Verantwortlichen verarbeiteten personenbezogenen Daten mitzuteilen und auszuüben.
- Erwartung – Die Verarbeitung sollte den berechtigten Erwartungen der betroffenen Personen entsprechen.
- Wahlmöglichkeiten der Verbraucher – Der Verantwortliche sollte seine Nutzer:innen nicht in unlauterer Weise an sich „binden“. Wenn es sich bei dem Dienst für die Verarbeitung personenbezogener Daten um einen proprietären Dienst handelt, kann eine dienstbezogene Bindung geschaffen werden; ein solcher Lock-in-Effekt kann unlauter sein, wenn er die Möglichkeit der betroffenen Personen beeinträchtigt, ihr Recht auf Datenübertragbarkeit nach Artikel 20 DS-GVO auszuüben.
- Kräfteverhältnis – Das Gleichgewicht der Kräfte sollte ein zentrales Ziel für das Verhältnis zwischen dem Verantwortlichen und der betroffenen Person sein. Ein Kräfteungleichgewicht sollte vermieden werden. Falls sich ein solches Ungleichgewicht nicht vermeiden lässt, sollte es anerkannt werden und es sollten geeignete Gegenmaßnahmen ergriffen werden.
- Keine Irreführung – Informationen über die Datenverarbeitung und Optionen zur Datenverarbeitung sollten objektiv und neutral bereitgestellt werden, wobei weder die Formulierungen noch die Gestaltung irreführend oder manipulativ sein sollten.
- Wahrhaftigkeit – Der Verantwortliche muss Informationen darüber bereitstellen, wie er personenbezogene Daten verarbeitet; er sollte sich bei seinen Handlungen seinem Wort entsprechend verhalten und die betroffenen Personen nicht in die Irre führen.

19. Bei der Bewertung irreführender Gestaltungsmuster ist es wichtig, die Einhaltung des Datenschutzes durch datenschutzfreundliche Voreinstellungen und durch Technikgestaltung zu bewerten, da die Einhaltung dazu führt, dass solche Gestaltungsmuster von vornherein vermieden werden. Die Konfrontation des eigenen Dienstes und der damit verbundenen Benutzeroberflächen mit Elementen, die Grundsätze des Datenschutzes durch datenschutzfreundliche Voreinstellungen und durch Technikgestaltung, wie beispielsweise die oben aufgeführten Grundsätze, beinhalten, wird dazu beitragen, vor der Inbetriebnahme des Dienstes dessen Aspekte zu ermitteln, die ein irreführendes Gestaltungsmuster darstellen würden. Wenn beispielsweise Datenschutzinformationen ohne Anwendung des Grundsatzes „Keine Irreführung“ bereitgestellt werden, besteht die Wahrscheinlichkeit, dass die Informationen ein irreführendes Gestaltungsmuster der Art **„Vor aller Augen verborgen“** oder **„Emotionale Steuerung“** darstellen, die beide im Anwendungsfall 1 näher ausgeführt werden.

3 LEBENSZYKLUS EINES NUTZERKONTOS IN SOZIALEN MEDIEN: PRAKTISCHE UMSETZUNG DER GRUNDSÄTZE

20. Die DS-GVO gilt für den gesamten Vorgang der automatisierten Verarbeitung personenbezogener Daten.²¹ Im Falle der Verarbeitung personenbezogener Daten im Rahmen des Betriebs von Social-Media-Plattformen hat dies zur Folge, dass die DS-GVO und ihre Grundsätze auf den gesamten Lebenszyklus eines Nutzerkontos Anwendung finden.

3.1 Eröffnung eines Nutzerkontos

Anwendungsfall 1: Registrierung eines Nutzerkontos

a. Beschreibung des Kontextes

21. Der erste Schritt, den die Nutzer:innen unternehmen müssen, um Zugang zu einer Social-Media-Plattform zu erhalten, ist die Einrichtung eines Kontos. Im Rahmen dieses Registrierungsverfahrens werden die Nutzer:innen aufgefordert, ihre personenbezogenen Daten wie Vor- und Nachname, E-Mail-Adresse oder mitunter ihre Telefonnummer anzugeben. Die Nutzer:innen müssen über die Verarbeitung ihrer personenbezogenen Daten informiert werden und werden in der Regel gebeten, zu bestätigen, dass sie die Datenschutzhinweise gelesen haben und in die Nutzungsbedingungen der Social-Media-Plattform einwilligen. Diese Informationen müssen in einer klaren, einfachen Sprache übermittelt werden, damit die Nutzer:innen sie leicht verstehen und bewusst zustimmen können.
22. In dieser ersten Phase des Anmeldeprozesses sollten die Nutzer:innen verstehen, wofür sie sich genau anmelden, und zwar in dem Sinne, dass der Gegenstand der Vereinbarung zwischen der Plattform und den Nutzer:innen so klar und eindeutig wie möglich beschrieben wird.
23. Daher müssen Social-Media-Anbieter den Datenschutz durch Technikgestaltung zum Schutz der Rechte und Freiheiten der betroffenen Personen wirksam berücksichtigen.²²

b. Maßgebliche Rechtsvorschriften

24. Social-Media-Anbieter müssen sicherstellen, dass sie bei der Gestaltung ihrer Benutzeroberflächen die Grundsätze nach Artikel 5 DS-GVO ordnungsgemäß umsetzen. Transparenz gegenüber den betroffenen Personen ist zwar stets von wesentlicher Bedeutung, im Stadium der Einrichtung eines Kontos bei einer Social-Media-Plattform gilt dies jedoch ganz besonders. Aufgrund ihrer Stellung als Verantwortliche oder Auftragsverarbeiter sollten Social-Media-Plattformen den Nutzer:innen bei ihrer Anmeldung die Informationen effizient und prägnant sowie klar getrennt von anderen, nicht datenschutzbezogenen Informationen übermitteln.²³ Ein Teil der Transparenzpflichten der Verantwortlichen besteht darin, die Nutzer:innen über ihre Rechte zu informieren, wobei eines dieser Rechte darin besteht, die Einwilligung jederzeit widerrufen zu können, wenn sie anwendbare Rechtsgrundlage darstellt.²⁴

i. Einwilligung im Stadium des Anmeldeverfahrens

²¹ Siehe Artikel 2 Absatz 1 der DS-GVO.

²² Siehe die Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.

²³ Siehe Leitlinien für Transparenz, Rn. 8.

²⁴ Leitlinien für Transparenz, Rn. 30 und S. 39.

25. Wie in Artikel 4 Nummer 11 und Artikel 7 DS-GVO dargelegt und durch Erwägungsgrund 32 klargestellt, muss die Einwilligung, wenn diese als Rechtsgrundlage für die Verarbeitung gewählt wird, eine „freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung [sein], mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“. Alle diese Voraussetzungen für eine Einwilligung müssen kumulativ erfüllt sein, damit sie als gültig angesehen werden kann.
26. Für Social-Media-Anbieter, die die Einwilligung der Nutzer:innen für unterschiedliche Verarbeitungszwecke einholen, bieten die EDSA-Leitlinien 5/2020 zur Einwilligung wertvolle Orientierungshilfen für die Einholung der Einwilligung.²⁵ Social-Media-Plattformen dürfen Bedingungen wie die Möglichkeit betroffener Personen, ihre Einwilligung freiwillig zu erteilen, nicht durch grafische Gestaltungen oder Formulierungen umgehen, mit denen die betroffenen Personen an der Ausübung dieses freien Willens gehindert werden. In diesem Zusammenhang heißt es in Artikel 7 Absatz 2 DS-GVO, dass das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen muss, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Nutzer:innen von Social-Media-Plattformen können während des Anmeldevorgangs und zu einem späteren Zeitpunkt über die Datenschutzeinstellungen ihre Einwilligung für Anzeigen oder besondere Analysen erteilen. In jedem Fall muss, wie in Erwägungsgrund 32 DS-GVO betont wird, die Einwilligung stets durch eine eindeutige bestätigende Handlung erteilt werden, sodass vorangekreuzte Kästchen oder Untätigkeit der Nutzer:innen keine Einwilligung darstellen.²⁶
27. Wie bereits in den EDSA-Leitlinien zur Einwilligung hervorgehoben wurde, muss es Mindestangaben geben, die den Nutzer:innen übermittelt werden, damit der Schwellenwert für die Einwilligung „in informierter Weise“ erreicht wird.²⁷ Ist dies nicht der Fall, kann die im Verlauf des Anmeldeverfahrens eingeholte Einwilligung nicht als gültig im Sinne der DS-GVO angesehen werden, sodass die Verarbeitung rechtswidrig ist.
28. Nutzer:innen werden um ihre Einwilligung zu unterschiedlichen Zwecken (z. B. Weiterverarbeitung personenbezogener Daten) gebeten. Eine Einwilligung ist nicht für einen bestimmten Fall erteilt und daher ungültig, wenn die Nutzer:innen keine klaren Informationen darüber erhalten, wozu sie ihre Einwilligung erteilen.²⁸ Wie in Artikel 7 Absatz 2 DS-GVO vorgesehen, sollte um die Einwilligung in einer Weise ersucht werden, die diese deutlich von anderen Informationen unterscheidet, unabhängig davon, wie der betroffenen Person die Informationen vorgelegt werden. Insbesondere wenn auf elektronischem Wege um die Einwilligung ersucht wird, darf diese Einwilligung nicht in den allgemeinen Geschäftsbedingungen enthalten sein.²⁹ Angesichts der Tatsache, dass immer mehr Nutzer:innen auf Social-Media-Plattformen zugreifen, die zur Anmeldung auf der Plattform die Benutzeroberfläche ihrer intelligenten Mobilgeräte nutzen, müssen die Anbieter der Art und Weise, in der um die Einwilligung ersucht wird, besondere Aufmerksamkeit widmen, um sicherzustellen, dass diese Einwilligung klar erkennbar ist. Die Nutzer:innen dürfen nicht mit einer übermäßigen Menge an Informationen konfrontiert werden, die sie dazu veranlasst, solche Informationen beim Lesen zu überspringen. Andernfalls kann es in Fällen, in denen Nutzer:innen bestätigen „müssen“, dass sie die

²⁵ EDSA-Leitlinien 5/2020 zur Einwilligung gemäß Verordnung 2016/679 Version 1.1 angenommen am 4. Mai 2020 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf.

²⁶ Siehe Urteil des Gerichtshofs der Europäischen Union vom 1. Oktober 2019, Verbraucherzentrale Bundesverband e.V./Planet 49 GmbH, Rechtssache C-673/17, Rn. 62-63.

²⁷ Leitlinien 5/2020 zur Einwilligung, Rn. 64; siehe auch den Anwendungsfall 3a in Teil 3.3 dieser Leitlinien.

²⁸ Siehe Leitlinien 5/2020 zur Einwilligung, Rn. 68.

²⁹ Leitlinien für Transparenz, Rn. 8.

gesamte Datenschutzerklärung gelesen haben und den allgemeinen Geschäftsbedingungen des Anbieters, einschließlich aller Verarbeitungsvorgänge, zustimmen, damit sie ein Konto erstellen können, als erzwungene Einwilligung in die darin aufgeführten besonderen Bedingungen angesehen werden. Führt die Ablehnung der Einwilligung zur Verweigerung des Dienstes, kann sie nicht als freiwillig, differenziert und für einen bestimmten Fall erteilt angesehen werden, wie es die DS-GVO verlangt. Eine Einwilligung, die mit der Annahme der Geschäftsbedingungen eines Anbieters „gebündelt“ wird, gilt nicht als „freiwillig erteilt“.³⁰ Dies ist auch der Fall, wenn der Verantwortliche die Bereitstellung eines Vertrags oder eines Dienstes mit dem Einwilligungsersuchen „verknüpft“, sodass er personenbezogene Daten verarbeitet, die für die Erfüllung des Vertrags durch den Verantwortlichen nicht erforderlich sind.

29. Während die Einwilligung durch eine konkrete Handlung seitens des Nutzers ausgedrückt werden muss, sollte das Fehlen der Einwilligung bis zu deren Erteilung als Grundzustand angesehen werden. Um die Ablehnung des Nutzers zum Ausdruck zu bringen, sollte daher keine Handlung seitens des Nutzers erforderlich sein oder sie sollte durch eine Handlung möglich sein, die genauso einfach ist wie die Handlung, mit der die Einwilligung zum Ausdruck gebracht werden kann.³¹

ii. Widerruf der Einwilligung – Artikel 7 Absatz 3 DS-GVO

30. Gemäß Artikel 7 Absatz 3 Satz 1 DS-GVO müssen die Nutzer:innen von Social-Media-Plattformen ihre Einwilligung jederzeit widerrufen können. Artikel 7 Absatz 3 Satz 3 DS-GVO entsprechend müssen Nutzer:innen vor Abgabe der Einwilligung auch auf das Recht hingewiesen werden, die Einwilligung zu widerrufen. Insbesondere müssen die Verantwortlichen nachweisen, dass Nutzer:innen die Möglichkeit haben, die Erteilung der Einwilligung zu verweigern oder die Einwilligung zu widerrufen, ohne dass dadurch Nachteile entstehen. Nutzer:innen von Social-Media-Plattformen, die mit einem Klick in die Verarbeitung ihrer personenbezogenen Daten einwilligen, indem sie beispielsweise ein Kästchen ankreuzen, müssen ihre Einwilligung auf ebenso einfache Weise widerrufen können.³² Dies unterstreicht, dass die Einwilligung eine reversible Entscheidung sein sollte, sodass die betroffene Person in Bezug auf die jeweilige Verarbeitung ein Maß an Kontrolle behält.³³ Der einfache Widerruf der Einwilligung stellt eine Voraussetzung für eine gültige Einwilligung nach Artikel 7 Absatz 3 Satz 4 der DS-GVO dar und sollte ohne Absenkung des Leistungsniveaus möglich sein.³⁴ Beispielsweise kann die Einwilligung nach der DS-GVO nicht als gültig angesehen werden, wenn sie lediglich durch einen Mausklick, Wischvorgang oder Tastenanschlag eingeholt wird, der Widerruf jedoch mehr Schritte erfordert,³⁵ schwieriger zu bewerkstelligen ist oder mehr Zeit in Anspruch nimmt.

c. Irreführende Gestaltungsmuster

³⁰ Siehe Leitlinien 8/2020 über die gezielte Ansprache von Nutzer:innen sozialer Medien, Rn. 57.

³¹ Siehe Erwägungsgrund 42 Satz 5 der DS-GVO.

³² Siehe Leitlinien für Transparenz, Rn. 113 ff.

³³ Leitlinien 5/2020 zur Einwilligung, Rn. 10.

³⁴ Leitlinien 5/2020 zur Einwilligung, Rn. 114.

³⁵ Siehe Leitlinien 5/2020 zur Einwilligung, Rn. 114.

31. Mehrere Bestimmungen der DS-GVO betreffen das Anmeldeverfahren. Daher gibt es eine Reihe irreführender Gestaltungsmuster, die gegeben sein können, wenn Social-Media-Anbieter die DS-GVO nicht in geeigneter Weise umsetzen.

i. Inhaltsbezogene Muster

Überfrachtung – Ständige Aufforderungen (Anhang I Checkliste 4.1.1)

32. Das irreführende Gestaltungsmuster **Ständige Aufforderungen** liegt vor, wenn Nutzer:innen dazu gedrängt werden, für die Zwecke der Verarbeitung mehr personenbezogene Daten als erforderlich bereitzustellen oder einer weiteren Verwendung ihrer Daten zuzustimmen, indem sie wiederholt gebeten werden, zusätzliche Daten zur Verfügung zu stellen oder in einen Verarbeitungszweck einzuwilligen. Solche wiederholten Aufforderungen können über ein oder mehrere Geräte erfolgen. Nutzer:innen neigen dazu, dem nachzugeben, weil sie dessen überdrüssig sind, bei jeder Nutzung der Plattform die Anfrage ablehnen zu müssen.

Beispiel 1:

Variante A: Im ersten Schritt des Anmeldeverfahrens müssen die Nutzer:innen zwischen verschiedenen Optionen für ihre Registrierung wählen. Sie können entweder eine E-Mail-Adresse oder eine Telefonnummer angeben. Entscheiden sich Nutzer:innen für die E-Mail-Adresse, versucht der Anbieter weiterhin, die Nutzer:innen davon zu überzeugen, dass sie ihre Telefonnummer angeben; dabei erklärt er, dass die Telefonnummer für Zwecke der Kontosicherheit genutzt werden wird, stellt aber keine Alternativen zu den Daten bereit, die von den Nutzer:innen übermittelt werden könnten oder bereits übermittelt wurden. Konkret öffnen sich während des Anmeldeprozesses mehrere Fenster mit einem Feld für die Telefonnummer sowie der Erläuterung „Wir verwenden Ihre [Telefon-]Nummer für Kontosicherheit“. Obwohl die Nutzer:innen das Fenster schließen können, werden sie dadurch überlastet und geben schließlich auf, indem sie ihre Telefonnummer angeben.

Variante B: Ein anderer Social-Media-Anbieter fordert die Nutzer:innen wiederholt, immer wenn sie sich in ihr Konto einloggen, zur Angabe ihrer Telefonnummer auf, obwohl sich die Nutzer:innen zuvor – während des Anmeldeverfahrens oder beim letzten Login – geweigert haben, die Telefonnummer anzugeben.

33. Das vorstehende Beispiel veranschaulicht eine Situation, in der Nutzer:innen ständig aufgefordert werden, bestimmte personenbezogene Daten, z. B. ihre Telefonnummer, anzugeben. Während diese **ständige Aufforderung** in Variante A des Beispiels mehrmals während des Anmeldeverfahrens erfolgt, zeigt Variante B, dass Nutzer:innen auch dann, wenn sie sich bereits angemeldet haben, mit diesem irreführenden Gestaltungsmuster konfrontiert werden können. Wichtig für die Vermeidung dieses irreführenden Gestaltungsmusters ist, den Grundsätzen der Datenminimierung nach Artikel 5 Absatz 1 Buchstabe c DS-GVO und in Fällen wie dem in Beispiel 1 Variante A beschriebenen auch dem Grundsatz der Zweckbindung nach Artikel 5 Absatz 1 Buchstabe b DS-GVO besonders sorgfältig Rechnung zu tragen. Wenn Social-Media-Anbieter also erklären, dass sie die Telefonnummer „zur Kontosicherheit“ verwenden werden, dürfen sie die Telefonnummer nur für die genannten Sicherheitszwecke verarbeiten und nicht in einer Weise, die über diesen ursprünglichen Zweck hinausgeht.

34. Um den Grundsatz der Datenminimierung zu wahren, sind Social-Media-Anbieter verpflichtet, keine zusätzlichen Daten wie die Telefonnummer anzufordern, wenn die Daten, die Nutzer:innen bereits während des Anmeldeverfahrens bereitgestellt haben, ausreichen. Um beispielsweise die Kontosicherheit zu gewährleisten, ist eine erweiterte Authentifizierung ohne die Telefonnummer möglich, indem einfach ein Code an das E-Mail-Konto des Nutzers gesendet wird oder verschiedene andere Instrumente genutzt werden.
35. Social-Media-Anbieter sollten sich daher auf Sicherheitsinstrumente stützen, die Nutzer:innen einfacher erneut aktivieren können. Beispielsweise kann der Anbieter den Nutzer:innen über einen zusätzlichen Kommunikationskanal wie z. B. eine Sicherheits-App, die die Nutzer:innen zuvor auf ihren Mobiltelefonen installiert haben, eine Authentifizierungsnummer übermitteln, ohne dass die Mobiltelefonnummern der Nutzer:innen erforderlich sind. Auch eine Nutzerauthentifizierung über eine E-Mail-Adresse ist weniger einschneidend als über eine Telefonnummer, da die Nutzer:innen einfach eine neue E-Mail-Adresse speziell für das Anmeldeverfahren einrichten und diese E-Mail-Adresse hauptsächlich im Zusammenhang mit dem sozialen Netzwerk nutzen könnten. Eine Telefonnummer lässt sich jedoch nicht so leicht austauschen, da es sehr unwahrscheinlich ist, dass Nutzer:innen nur aus Gründen der Authentifizierung eine neue SIM-Karte kaufen oder einen neuen Telefonvertrag abschließen würden.
36. Hier ist zu berücksichtigen, dass das Ziel einer solchen Bitte, wenn es darin besteht, zu beweisen, dass sich das zum Einloggen in das soziale Netzwerk verwendete Gerät rechtmäßig im Besitz des Nutzers befindet, mit unterschiedlichen Mitteln erreicht werden kann und eine Telefonnummer nur eines von ihnen ist. Daher kann eine Telefonnummer nur eine maßgebliche, freiwillig genutzte Option für Nutzer:innen sein. Letztendlich müssen die Nutzer:innen entscheiden, ob sie dieses Mittel als Authentifizierungsfaktor verwenden möchten. Insbesondere werden für eine einmalige Überprüfung keine Telefonnummern der Nutzer:innen benötigt, da die E-Mail-Adresse der Anknüpfungspunkt für die reguläre Kontaktaufnahme während des Registrierungsverfahrens ist.
37. Die unter Beispiel 1 Variante A dargestellte Praxis kann die Nutzer:innen irreführen und dazu verleiten, Informationen dieser Art unfreiwillig zu übermitteln, da sie meinen, dass dies für die Aktivierung oder den Schutz des Kontos erforderlich ist. In Wirklichkeit erhielten die Nutzer:innen jedoch nie eine Alternative (z. B. Nutzung der E-Mail zur Aktivierung des Kontos und zu Sicherheitszwecken). In Beispiel 1 Variante B werden die Nutzer:innen nicht über den Verarbeitungszweck informiert. Diese Variante stellt jedoch nach wie vor ein irreführendes Gestaltungsmuster in Form von **ständigen Aufforderungen** dar, da der Social-Media-Anbieter nicht berücksichtigt, dass die Nutzer:innen zuvor die Angabe der Telefonnummer verweigerten, sondern weiterhin ständig danach fragt. Wenn bei den Nutzer:innen der Eindruck entsteht, dass sie dieses wiederholte Ersuchen nur durch die Eingabe ihrer Daten vermeiden können, werden sie wahrscheinlich nachgeben.
38. Im folgenden Beispiel werden die Nutzer:innen wiederholt animiert, der Social-Media-Plattform Zugang zu ihren Kontaktdaten zu gewähren.

Beispiel 2: Eine Social-Media-Plattform verwendet ein Informations- oder Fragezeichen-Symbol als Anreiz, damit Nutzer:innen die aktuell erbetene „optionale“ Handlung vornehmen. Statt Nutzer:innen, die von diesen Schaltflächen Hilfe erwarten, lediglich Informationen bereitzustellen, werden die Nutzer:innen auf der Plattform aufgefordert, ihre Kontaktdaten von ihrem E-Mail-Konto zu importieren, indem sich wiederholt ein Dialogfenster mit der Aussage „Los geht’s“ öffnet.

39. Insbesondere in der Phase des Anmeldeverfahrens können diese **ständigen Aufforderungen** Nutzer:innen dazu veranlassen, zum endgültigen Abschluss ihrer Registrierung der Aufforderung der Plattform nachzukommen. Die Wirkung dieses irreführenden Gestaltungsmusters wird noch verstärkt, wenn es, wie in diesem Beispiel, mit motivierenden Formulierungen kombiniert wird, die zusätzlich ein Gefühl der Dringlichkeit entstehen lassen.
40. Eine Auseinandersetzung mit den beeinflussenden Wirkungen von Formulierungen und visuellen Darstellungen erfolgt nachstehend im Zusammenhang mit der Prüfung des irreführenden Gestaltungsmusters **Emotionale Steuerung**.³⁶

Behindern – Irreführende Handlung (Anhang I Checkliste 4.4.3)

41. Ein weiteres Beispiel für eine Situation, in der Social-Media-Anbieter die Telefonnummern der Nutzer:innen anfordern, ohne dass dies notwendig ist, betrifft die Nutzung der App der Plattform.

Beispiel 3: Wenn sich Nutzer:innen über einen Desktop-Browser bei einer Social-Media-Plattform anmelden, werden sie eingeladen, auch die mobile App der Plattform zu nutzen. Während eines Vorgangs, der wie ein weiterer Schritt im Anmeldeverfahren aussieht, werden die Nutzer:innen eingeladen, die App zu entdecken. Wenn sie dann in der Erwartung, zu einem App-Store weitergeleitet zu werden, das Symbol anklicken, werden sie stattdessen gebeten, ihre Telefonnummer anzugeben, damit sie eine Textnachricht mit dem Link zur App erhalten können.

42. Nutzer:innen zu erklären, dass sie die Telefonnummer angeben müssen, um einen Link zum Herunterladen der App zu erhalten, stellt aus einer Reihe von Gründen eine **irreführende Handlung** dar: Zunächst gibt es mehrere Möglichkeiten für die Nutzung einer App, z. B. durch Scannen eines QR-Codes, die Nutzung eines Links oder Herunterladen der App aus dem App-Store. Zweitens zeigen diese Alternativen, dass es für den Anbieter keinen zwingenden Grund gibt, die Telefonnummer des Nutzers anzufordern. Wenn die Nutzer:innen das Anmeldeverfahren abgeschlossen haben, müssen sie ihre Login-Daten (d. h. in der Regel E-Mail-Adresse und Passwort) nutzen können, um sich unabhängig vom verwendeten Gerät einzuloggen, also ungeachtet dessen, ob sie einen Desktop-Browser, einen Browser für Mobilgeräte oder eine App verwenden. Dies wird umso deutlicher durch die Tatsache, dass Nutzer:innen wünschen könnten, die App nicht auf einem Smartphone, sondern stattdessen auf ihrem Tablet zu installieren, das nicht mit einer Telefonnummer verknüpft ist.

Aufwühlen – Emotionale Steuerung (Anhang I Checkliste 4.3.1)

43. Mit dem irreführenden Gestaltungsmuster **Emotionale Steuerung** werden Formulierungen oder visuelle Elemente (z. B. Stil, Farben, Bilder usw.) so verwendet, dass den Nutzer:innen Informationen entweder mit einer sehr positiven Art und Weise vermittelt werden, sodass sich die Nutzer:innen gut, sicher oder belohnt fühlen, oder aber mit einer stark negativen Art und Weise, die dazu führt, dass sich die Nutzer:innen ängstlich, schuldig oder bestraft fühlen. Die Art, wie Nutzer:innen Informationen präsentiert werden, beeinflusst ihren emotionalen Zustand in einer Weise, die sie wahrscheinlich dazu verleitet, in einer Weise zu handeln, die ihren Datenschutzinteressen zuwiderläuft. Die Auswirkungen solcher Praktiken können noch effektiver sein, wenn sie auf Daten beruhen, die von der Plattform

³⁶ Siehe Rn. 43 ff. im Anwendungsfall 1 sowie die Übersicht über Beispiele in der Checkliste im Anhang.
Angenommen

erhoben wurden. Die Einflussnahme auf Entscheidungen mittels Bereitstellung verzerrter Informationen an Einzelpersonen kann im Allgemeinen als unlautere Praxis angesehen werden, die dem in Artikel 5 Absatz 1 Buchstabe a DS-GVO verankerten Grundsatz der Verarbeitung nach Treu und Glauben zuwiderläuft. Sie kann während des gesamten Nutzererlebnisses auf einer Social-Media-Plattform stattfinden. In der Phase des Anmeldeverfahrens kann die Lenkungswirkung jedoch besonders stark sein, wenn man bedenkt, dass die Nutzer:innen zusätzlich zu den Schritten, die für den Abschluss der Registrierung erforderlich sind, möglicherweise eine übergroße Menge an Informationen zu bewältigen haben.

44. In Anbetracht dessen, dass sie als betroffene Personen besonders schutzbedürftig sind, kann **Emotionale Steuerung** im Stadium der Registrierung bei einer Social-Media-Plattform auf Kinder, ältere Menschen und andere Gruppen sogar noch größere Auswirkungen haben (d. h. sie stellen aufgrund ihrer mangelnden Kenntnisse von Verarbeitungstätigkeiten mehr personenbezogene Daten bereit).³⁷ Wenn sich Plattformdienste sozialer Medien an Kinder oder andere schutzbedürftige betroffene Personen richten, sollten sie sicherstellen, dass die verwendete Sprache, einschließlich Ton und Stil, angemessen ist, damit die schutzbedürftigen Nutzer:innen als Empfänger der Nachricht die übermittelten Informationen leicht verstehen können.³⁸ Angesichts der Schutzbedürftigkeit von Kindern, älteren Menschen und anderen betroffenen Personen können irreführende Gestaltungsmuster diese Nutzer:innen dazu veranlassen, mehr Informationen preiszugeben, da sie sich durch eine „befehlende“ Ausdruckweise hierzu verpflichtet fühlen können, beispielsweise um bei Mitgliedern ihrer Bezugsgruppe beliebt zu erscheinen oder weil sie meinen, dass die Bereitstellung der Daten obligatorisch ist.
45. Werden Nutzer:innen von Social-Media-Plattformen aufgefordert, ihre Daten rasch preiszugeben, haben sie keine Zeit, die Informationen, die sie erhalten haben, zu „verarbeiten“ und somit tatsächlich zu verstehen, um eine bewusste Entscheidung treffen zu können. Die von Social-Media-Plattformen verwendete motivierende Sprache könnte Nutzer:innen dazu veranlassen, in der Folge mehr Daten als erforderlich bereitzustellen, wenn sie meinen, dass das, was von der Plattform vorgeschlagen wird, das ist, was die meisten Nutzer:innen tun, und somit der „korrekten Vorgehensweise“ entspricht.

Beispiel 4: Die Social-Media-Plattform fordert Nutzer:innen mit der folgenden Aussage auf, ihren geografischen Standort mitzuteilen: „Hey, bist Du ein einsamer Wolf? Aber Information zu teilen und Verbindungen zu Anderen zu suchen macht die Welt zu einem besseren Ort! Teile Deinen geografischen Standort! Lass Dich von den Orten und Menschen um Dich herum inspirieren!“

46. Während des Anmeldeverfahrens besteht das Ziel der Nutzer:innen darin, die Registrierung abzuschließen, um die Social-Media-Plattform nutzen zu können. Irreführende Gestaltungsmuster wie **Emotionale Steuerung** wirken sich in diesem Zusammenhang stärker aus. Es besteht die Gefahr, dass sie in der Mitte oder gegen Ende des Anmeldeprozesses stärker sind als zu Beginn, da die Nutzer:innen meist alle erforderlichen Schritte „auf die Schnelle“ abschließen, oder anfälliger für ein Gefühl der Dringlichkeit sind. Vor diesem Hintergrund besteht eine höhere Wahrscheinlichkeit, dass Nutzer:innen alle geforderten Daten bereitstellen, ohne sich Zeit für die Frage zu nehmen, ob sie dies tun sollten. In diesem Sinne kann die vom Social-Media-Anbieter verwendete motivierende Sprache Einfluss auf die spontane Entscheidung der Nutzer:innen haben, ebenso wie die Kombination motivierender Sprache mit anderen Formen der Betonung wie Ausrufezeichen; siehe dazu das folgende Beispiel.

³⁷ Siehe auch Rn. 7.

³⁸ Siehe Leitlinien für Transparenz, Rn. 18.

Beispiel 5: Social-Media-Anbieter schaffen Anreize für Nutzer:innen, um sie dazu zu bewegen, mehr personenbezogene Daten weiterzugeben, als es tatsächlich erforderlich ist, indem sie die Nutzer:innen zu einer Beschreibung über sich selbst auffordern: *„Erzähle uns etwas über Deine umwerfende Persönlichkeit! Wir können es kaum erwarten. Also los, lass es uns wissen!“*

47. Mit dieser Praxis erhalten Social-Media-Plattformen detailliertere Profile ihrer Nutzer:innen. Je nach Fall ist jedoch die Bereitstellung von mehr personenbezogenen Daten, z. B. über die Persönlichkeit der Nutzer:innen, für die Nutzung des Dienstes an sich möglicherweise nicht erforderlich und verstößt daher gegen den Grundsatz der Datenminimierung nach Artikel 5 Absatz 1 Buchstabe c DS-GVO. Wie in Beispiel 5 veranschaulicht, fördern solche Techniken nicht den freien Willen der Nutzer:innen zur Bereitstellung ihrer Daten, da die verwendete anordnende Sprache dazu führen kann, dass sich die Nutzer:innen verpflichtet fühlen, eine Selbstbeschreibung bereitzustellen, weil sie bereits Zeit in die Registrierung investiert haben und diese abschließen möchten. Wenn sich Nutzer:innen im Prozess der Registrierung bei einem Konto befinden, nehmen sie sich weniger Zeit, über die Beschreibung, die sie geben, nachzudenken oder sogar zu überlegen, ob sie überhaupt eine Beschreibung geben wollen. Dies ist insbesondere dann der Fall, wenn die verwendete Sprache ein Gefühl der Dringlichkeit vermittelt oder wie ein Imperativ klingt. Wenn die Nutzer:innen dieses Gefühl der Verpflichtung selbst dann haben, wenn die Bereitstellung der Daten in Wirklichkeit nicht obligatorisch ist, kann dies Auswirkungen auf ihren „freien Willen“ haben. Dies bedeutet auch, dass die von der Social-Media-Plattform bereitgestellten Informationen unklar waren.

Beispiel 6: Der Teil des Anmeldeverfahrens, in dem Nutzer:innen aufgefordert werden, ihr Bild hochzuladen, enthält eine Schaltfläche „?“. Wenn man sie anklickt, erscheint folgende Meldung: *„Du musst nicht erst zum Friseur gehen. Wähle einfach ein Foto aus, das zum Ausdruck bringt: ‚Das bin ich‘“.*

48. Auch wenn die Sätze in Beispiel 6 darauf abzielen, Nutzer:innen zu motivieren und das Verfahren scheinbar zu vereinfachen (d. h. die Anmeldung erfordert kein offizielles Foto), können sich solche Praktiken auf die abschließende Entscheidung der Nutzer:innen auswirken, die ursprünglich beschlossen hatten, für ihr Konto kein Bild zu übermitteln. Fragezeichen werden für Fragen verwendet, und wenn sie als Symbol erscheinen, können Nutzer:innen beim Anklicken hilfreiche Informationen erwarten. Wenn diese Erwartung nicht erfüllt wird und die Nutzer:innen stattdessen erneut aufgefordert werden, die Handlungen vorzunehmen, denen sie zurückhaltend gegenüberstehen, wäre die ohne Information der Nutzer:innen über die Verarbeitung ihres Bildes eingeholte Einwilligung ungültig, da die Anforderungen an eine „in informierter Weise“ und „freiwillig erteilte“ Einwilligung nach Artikel 7 DS-GVO in Verbindung mit Artikel 4 Nummer 11 DS-GVO nicht erfüllt wären. Der Faktor der Emotionen hat folglich einen starken Einfluss auf die Wirksamkeit der Einwilligung.

Behindern – Länger als erforderlich (Anhang I Checkliste 4.4.2)

49. Wenn Nutzer:innen versuchen, eine datenschutzbezogene Kontrollfunktion zu aktivieren, das Nutzererlebnis aber so gestaltet ist, dass die Nutzer:innen mehr Schritte unternehmen müssen, als für die Aktivierung dateninvasiver Optionen erforderlich ist, stellt dies das irreführende Gestaltungsmuster ***Länger als erforderlich*** dar. Dieses Muster dürfte Nutzer:innen davon abhalten, die datenschutzbezogenen Kontrollen zu aktivieren. Im Anmeldeverfahren kann dies in der Form erfolgen, dass ein Pop-in- oder Pop-up-Fenster angezeigt wird, in dem Nutzer:innen aufgefordert werden, ihre Entscheidung zu bestätigen, wenn sie sich für eine restriktive Option entscheiden (z. B. indem sie ihre

Profile als private Profile anlegen). Das nachstehende Beispiel veranschaulicht einen weiteren Fall, in dem ein Anmeldeverfahren ***länger als erforderlich*** dauert.

Beispiel 7: Während des Anmeldevorgangs wird Nutzer:innen, die auf die Schaltflächen „Überspringen“ klicken, um zu vermeiden, dass bestimmte Arten von Daten eingegeben werden, ein Pop-up-Fenster angezeigt, in dem „*Bist Du sicher?*“ gefragt wird. Indem ihre Entscheidung in Frage gestellt wird und daher Zweifel in ihnen geweckt werden, regen die Anbieter die Nutzer:innen an, ihre Entscheidung zu überprüfen und diese Arten von Daten, beispielsweise ihr Geschlecht, ihre Kontaktliste oder ihr Bild, offenzulegen. Dagegen sehen Nutzer:innen, die sich für die direkte Eingabe der Daten entscheiden, keine Nachricht, in der sie zum Überdenken ihrer Wahl aufgefordert werden.

Werden Nutzer:innen um eine Bestätigung gebeten, dass sie ein Datenfeld nicht ausfüllen möchten, kann sie das veranlassen, ihre ursprüngliche Entscheidung rückgängig zu machen und die geforderten Daten einzugeben. Dies trifft besonders auf Nutzer:innen zu, die mit den Funktionen von Social-Media-Plattformen nicht vertraut sind. Mit diesem als ***Länger als erforderlich*** bezeichneten irreführenden Gestaltungsmuster wird versucht, Einfluss auf die Entscheidungen von Nutzer:innen zu nehmen, indem sie aufgehalten werden und ihre ursprüngliche Wahl infrage gestellt wird, zusätzlich zu einer unnötigen Verlängerung des Anmeldeverfahrens. Dies stellt einen Verstoß gegen den Grundsatz der Verarbeitung nach Treu und Glauben gemäß Artikel 5 Absatz 1 Buchstabe a DS-GVO dar. Das Beispiel zeigt, dass das irreführende Gestaltungsmuster die Nutzer:innen dazu bringen kann, (mehr) personenbezogene Daten offenzulegen, als sie ursprünglich beschlossen hatten. Es beschreibt ein Ungleichgewicht der Behandlung von Nutzer:innen, die ihre personenbezogenen Daten sofort offenlegen, und solchen, die dies nicht tun. Nur diejenigen, die die Offenlegung der Daten verweigern, werden aufgefordert, ihre Entscheidung zu bestätigen, während Nutzer:innen, die die Daten offenlegen, nicht zur Bestätigung ihrer Entscheidung aufgefordert werden. In Bezug auf Nutzer:innen, die diese personenbezogenen Daten nicht offenlegen wollen, stellt dies einen Verstoß gegen den Grundsatz der Verarbeitung nach Treu und Glauben gemäß Artikel 5 Absatz 1 Buchstabe a DS-GVO dar.

ii. Oberflächenbezogene Muster

Aufwühlen – Vor aller Augen verborgen (Anhang I Checkliste 4.3.2)

50. Dem Grundsatz der Transparenz entsprechend müssen betroffenen Personen klare Informationen bereitgestellt werden, damit sie in die Lage versetzt werden, zu verstehen, wie ihre personenbezogenen Daten verarbeitet werden und wie sie diese kontrollieren können. Darüber hinaus müssen diese Informationen für die betroffenen Personen leicht erkennbar sein. Informationen zum Datenschutz, insbesondere Links, werden jedoch häufig so angezeigt, dass sie von den Nutzer:innen leicht übersehen werden. Bei solchen Praktiken des Typs ***Vor aller Augen verborgen*** wird für Informationen oder Kontrollfunktionen bezüglich des Datenschutzes ein Grafikformat verwendet, das Nutzer:innen einen „Anreiz“ weg von Optionen, die für den Datenschutz vorteilhaft sind, hin zu weniger restriktiven und somit stärker invasiven Optionen gibt.
51. Die Verwendung einer kleinen Schriftgröße oder einer Farbe, die nicht kontrastreich genug ist, um eine ausreichende Lesbarkeit zu ermöglichen (z. B. hellgraue Textfarbe auf weißem Hintergrund), kann sich negativ auf die Nutzer:innen auswirken, da der Text weniger sichtbar ist und die Nutzer:innen ihn

entweder übersehen oder Schwierigkeiten haben, ihn zu lesen. Dies ist insbesondere dann der Fall, wenn neben den obligatorischen datenschutzbezogenen Informationen ein oder mehrere auffällige Elemente platziert werden. Diese Techniken auf den Benutzeroberflächen führen die Nutzer:innen in die Irre und lassen die Erkennung von Informationen, die mit dem Schutz ihrer Daten zusammenhängen, beschwerlicher und zeitaufwendiger werden, da mehr Zeit und Gründlichkeit benötigt werden, um die maßgeblichen Informationen ausfindig zu machen.

Beispiel 8: Unmittelbar nach Abschluss der Registrierung können die Nutzer:innen nur auf die Datenschutzinformationen zuzugreifen, indem sie das allgemeine Menü der Social-Media-Plattform aufrufen und den Abschnitt des Untermenüs durchsuchen, der einen Link zu „*Datenschutz und Dateneinstellungen*“ enthält. Bei einem Besuch dieser Seite ist ein Link zur Datenschutzerklärung nicht auf den ersten Blick sichtbar. Die Nutzer:innen müssen in einer Ecke der Seite ein winziges Symbol wahrnehmen, das auf die Datenschutzerklärung hinweist; dies bedeutet, dass die Nutzer:innen kaum erkennen können, wo sich die Informationen über die Datenschutzbestimmungen befinden.

52. In diesem Zusammenhang ist zu betonen, dass auch dann, wenn Social-Media-Anbieter den betroffenen Personen alle gemäß Artikel 13 und 14 DS-GVO bereitzustellenden Informationen zur Verfügung stellen, die Art und Weise, wie diese Informationen dargestellt werden, immer noch gegen die übergeordneten Transparenzanforderungen nach Artikel 12 Absatz 1 DS-GVO verstoßen kann. Wenn die Informationen **vor aller Augen verborgen** sind und daher wahrscheinlich übersehen werden, führt dies zu Verwirrung oder Orientierungslosigkeit und kann entgegen Artikel 12 Absatz 1 DS-GVO nicht als verständlich und leicht zugänglich angesehen werden.
53. Das obige Beispiel zeigt zwar das irreführende Gestaltungsmuster nach Abschluss des Anmeldeverfahrens, aber dieses Muster tritt auch bereits während des Anmeldeverfahrens auf. Dies wird aus dem nachstehenden Beispiel ersichtlich, in dem die Gestaltungsmuster **Vor aller Augen verborgen** und **Trügerische Bequemlichkeit** miteinander kombiniert werden.

Überspringen – Trügerische Bequemlichkeit (Anhang I Checkliste 4.2.1)

54. Social-Media-Anbieter müssen auch den Grundsatz des Datenschutzes durch datenschutzfreundliche Voreinstellungen beachten. Bei der Vorauswahl von Dateneinstellungen unterliegen die Nutzer:innen einem bestimmten Datenschutzniveau, das der Anbieter mittels Voreinstellung festlegt und das nicht von den Nutzer:innen bestimmt wird. Darüber hinaus wird den Nutzer:innen nicht immer sofort die Möglichkeit geboten, die Einstellungen in strengere, datenschutzkonforme Einstellungen zu ändern. Die Einhaltung der DS-GVO in dieser Hinsicht bedeutet nicht, dass alle Optionen genau gleich aussehen müssen. Wenn Anbieter jedoch eine der Optionen hervorheben und somit die Aufmerksamkeit der Nutzer:innen auf sie lenken, muss dies im Hinblick auf personenbezogene Daten die restriktivste Option sein, damit unter anderem dem Grundsatz der Datenminimierung nach Artikel 5 Absatz 1 Buchstabe c DS-GVO entsprochen wird.
55. Wenn die dateninvasivsten Merkmale und Optionen per Voreinstellung aktiviert sind, stellt dies das Muster **Trügerische Bequemlichkeit** dar. Aufgrund des Voreinstellungseffektes, der Personen dazu drängt, eine vorab ausgewählte Option beizubehalten, ist es unwahrscheinlich, dass die Nutzer:innen diese ändern, selbst wenn sie die Möglichkeit dazu erhalten. Wie in Beispiel 9 veranschaulicht, ist diese Praxis häufig in Anmeldeverfahren anzutreffen, da sie eine wirksame Möglichkeit ist, dateninvasive

Optionen zu aktivieren, die Nutzer:innen andernfalls wahrscheinlich ablehnen würden. Solche irreführenden Gestaltungsmuster stehen im Widerspruch zum Grundsatz des Datenschutzes durch datenschutzfreundliche Voreinstellungen gemäß Artikel 25 Absatz 2 DS-GVO, insbesondere wenn sie sich auf die Erhebung personenbezogener Daten, den Umfang der Verarbeitung, den Zeitraum der Datenspeicherung und die Zugänglichkeit der Daten auswirken.³⁹

Sign-up

Just one more step to join your friends!

Your birthdate

Day Month Year

29 12 1996

Share it with no one

Share it with my friends

Share it with everyone

Join the network!

[Skip this step and sign up](#)

Beispiel 9: In diesem Beispiel Nutzer:innen können die Nutzer:innen bei der Eingabe ihres Geburtsdatums entscheiden, an wen sie diese Informationen weitergeben wollen. Während weniger invasive Optionen zur Verfügung stehen, ist standardmäßig die Option „Für alle freigeben“ ausgewählt, was bedeutet, dass alle, d. h. sowohl registrierte Nutzer:innen als auch sonstige Internetnutzer, das Geburtsdatum der Nutzer:innen sehen können.

56. Beispiel 9 zeigt ein Muster des Typs **Trügerische Bequemlichkeit**, da nicht die Option, die das höchste Niveau an Datenschutz bietet, als Voreinstellung ausgewählt und somit aktiviert ist. Darüber hinaus wirkt der Voreinstellungseffekt dieses Musters bei den Nutzer:innen als Anstoß, die Vorauswahl

³⁹ Siehe auch Rn. 446 der endgültigen Entscheidung der irischen Datenschutzbehörde zu Instagram (Meta Platforms Ireland Limited) im Anschluss an den verbindlichen Streitbeilegungsbeschluss des EDSA vom 28. Juli 2022, https://edpb.europa.eu/news/news/2022/record-fine-instagram-following-edpb-intervention_de.

beizubehalten, sich also in dieser Phase weder die Zeit zu nehmen, die anderen Optionen zu prüfen, noch die Einstellung zu einem späteren Zeitpunkt zu ändern. In dieser Benutzeroberfläche wird außerdem das Muster **Vor aller Augen verborgen** verwendet. In der Tat ist die Eingabe des Geburtsdatums nicht obligatorisch, da die Nutzer:innen diesen Anmeldeschritt überspringen können, indem sie auf den Link „*Diesen Schritt überspringen und anmelden*“ klicken, der unter der Schaltfläche „*Werde Teil des Netzwerks!*“ verfügbar ist. Aufgrund der Tatsache, dass das Feld für das Geburtsdatum und die Schaltfläche für die Bestätigung so hervorstechen, besteht die Wahrscheinlichkeit, dass die Nutzer:innen dazu gebracht werden, ihr Geburtsdatum einzugeben und an das soziale Netzwerk zu senden, weil sie die Möglichkeit, diese Information nicht weiterzugeben, nicht bemerken. Dieser Effekt wäre noch stärker, wenn neben dem Feld und der Schaltfläche animierte Kreise verwendet würden, die die Aufmerksamkeit der Nutzer:innen stark auf sich ziehen.

57. Die Achtung des Grundsatzes des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen bedeutet nicht, dass alle angebotenen Optionen genau gleich aussehen müssen. Wenn Verantwortliche jedoch beschließen, eine Option stärker hervorzuheben als die andere(n), muss die hervorgehobene Option hinsichtlich der Datenverarbeitung die restriktivste Option sein.
58. Abgesehen davon, dass Nutzer:innen dazu gebracht werden, eine Option beizubehalten, die nicht unbedingt ihren Präferenzen entspricht, kann auch der Fall eintreten, dass die Social-Media-Anbieter nach Abschluss des Anmeldeverfahrens die Nutzer:innen möglicherweise nicht auffordern, ihre Datenschutzeinstellungen zu überprüfen oder ihren Präferenzen entsprechend zu ändern. Darüber hinaus könnte die Änderung dieser Standardeinstellungen mehrere Schritte erfordern. Werden Nutzer:innen nicht in irgendeiner Weise aufgefordert, ihre Datenschutzeinstellungen zu überprüfen bzw. zu ändern, oder werden sie nicht auf eine klare Art und Weise zu damit zusammenhängenden Informationen geleitet, wird das Niveau ihres Datenschutzes von ihrer eigenen Initiative abhängen. Um den Nutzer:innen die Kontrolle über ihre Daten zu erleichtern, können sogenannte Datenschutz-Dashboards verwendet werden, die diese Vorhaben zentralisieren und erleichtern sollen.
59. Es ist unbedingt zu bedenken, dass fehlender Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen in Verbindung mit dem oben beschriebenen Voreinstellungseffekt schädliche Folgen für die betroffenen Personen, einschließlich ihrer Cybersicherheit, haben kann. Die öffentliche Anzeige personenbezogener Daten wie des Geburtsdatums, das für Überprüfungsverfahren durch andere Online-Dienste verwendet wird, könnte Kriminellen den Zugang zu Einkaufs-, Bank- und sonstigen Konten der Nutzer:innen erleichtern. Eine weitere schädliche Folge sind Kontaktmöglichkeiten auf der Social-Media-Plattform: Wenn die Standardoption für die Übermittlung von Kontaktanfragen oder Nachrichten an Nutzer:innen auf „An alle“ gesetzt ist, erhöht sich das Risiko für Cyber-Grooming und Betrug, insbesondere bei schutzbedürftigen Gruppen.
60. Schließlich sind die in Artikel 4 Nummer 11 DS-GVO festgelegten Bedingungen für die Einwilligung nicht erfüllt und die Verarbeitung würde als rechtswidrig im Sinne von Artikel 5 Absatz 1 Buchstabe a und Artikel 6 Absatz 1 Buchstabe a DS-GVO gelten, wenn bei der Einholung der Einwilligung **Trügerische Bequemlichkeit** zum Einsatz kommt, beispielsweise wenn ein vorab angekreuztes Kästchen verwendet oder Inaktivität als Zustimmung ausgelegt wird, was der Annahme gleichkommt, dass Nutzer:innen standardmäßig einwilligen.

Behindern – Sackgasse (Anhang I Checkliste 4.4.1)

61. Hier ist der Hinweis wichtig, zu betonen, dass die Anmeldephase für die Nutzer:innen im Hinblick auf die Einholung von Informationen ein entscheidender Zeitpunkt ist. Wenn sie nach Informationen suchen und diese nicht finden können, weil kein Link für Weiterleitungen verfügbar ist oder dieser nicht funktioniert, stellt dies ein Gestaltungsmuster des Typs **Sackgasse** dar, weil Nutzer:innen ihr Ziel nicht erreichen können.

Beispiel 10: Den Nutzer:innen werden keine Links zu Datenschutzinformationen zur Verfügung gestellt, sobald sie mit dem Anmeldeverfahren begonnen haben. Die Nutzer:innen können diese Informationen nicht finden, da sie nirgendwo in der Anmelde-Oberfläche bereitgestellt werden, nicht einmal in einer Fußnote.

62. Dieses Beispiel hat in der Praxis zur Folge, dass Nutzer:innen nur die Möglichkeit haben, entweder die Registrierung zu stoppen und zur Startseite zurückzukehren, sofern diese einen Link zu den Datenschutzhinweisen enthält, oder aber die Registrierung abzuschließen, sich auf der Social-Media-Plattform anzumelden und erst dann auf datenschutzbezogene Informationen zugreifen zu können. Dies verstößt gegen den Grundsatz der Transparenz und des leichten Zugangs zu Informationen, die betroffenen Personen gemäß Artikel 12 Absatz 1 DS-GVO zu übermitteln sind. Das Beispiel erfüllt auch die Anforderungen von Artikel 13 Absätze 1 und 2 DS-GVO nicht, da zum Zeitpunkt der Erhebung personenbezogener Daten weder Informationen zur Verfügung gestellt werden noch zugänglich sind.
63. Das Gestaltungsmuster **Sackgasse** kann auch auf andere Weise auftreten, nämlich dann, wenn Nutzer:innen während des Anmeldeverfahrens eine datenschutzbezogene Handlung oder Option zur Verfügung gestellt wird, die sie später, wenn sie den Dienst nutzen, nicht mehr auffinden können.

Beispiel 11: Während des Anmeldeverfahrens können die Nutzer:innen in die Verarbeitung ihrer personenbezogenen Daten für Werbezwecke einwilligen, und sie werden darüber informiert, dass sie ihre Wahl nach der Registrierung jederzeit ändern können, indem sie zur Datenschutzerklärung navigieren. Sobald die Nutzer:innen das Registrierungsverfahren abgeschlossen haben und die Datenschutzerklärung aufsuchen, finden sie dort keine Möglichkeiten oder Hinweise für den Widerruf ihrer Einwilligung.

64. In diesem konkreten Beispiel haben Nutzer:innen keine Möglichkeit, ihre Einwilligung zu widerrufen, sobald sie sich angemeldet haben. Hier verletzt das irreführende Gestaltungsmuster **Sackgasse** das Recht der betroffenen Personen, ihre Einwilligung gemäß Artikel 7 Absatz 3 Sätze 1 und 4 DS-GVO jederzeit und so einfach wie bei der Erteilung der Einwilligung zu widerrufen.
65. Und schließlich ist der Hinweis auf einen Link, der Nutzer:innen vermeintlich zu datenschutzbezogenen Seiten wie Einstellungen oder Datenschutzinformationen führt, ein Beispiel für ein Gestaltungsmuster des Typs **Sackgasse**, wenn der Link defekt ist und keine alternativen Links zur Verfügung gestellt werden, auf die Nutzer:innen ausweichen können und die ihnen helfen, das Gesuchte zu finden. Auf diese Weise können die Nutzer:innen nicht nach relevanten Informationen suchen und sie erhalten keine Erläuterungen wie beispielsweise den Grund, warum dies der Fall ist (z. B. technische Probleme). In einem solchen Fall treten die gleichen Probleme im Zusammenhang mit der Transparenz und dem leichten Zugang zu Informationen auf, wie sie in Randnummer 58 beschrieben werden.

d. Best Practices

Hinsichtlich der Gestaltung von Benutzeroberflächen, die die wirksame Umsetzung der DS-GVO erleichtern, empfiehlt der EDSA die Anwendung der folgenden Best Practices für das Anmeldeverfahren:

Schnellzugriffe: Links zu Informationen, Handlungen oder Einstellungen, die Nutzer:innen bei der Verwaltung ihrer Daten und ihrer Datenschutzeinstellungen von praktischem Nutzen sein können, sollten überall dort verfügbar sein, wo die Nutzer:innen mit einer entsprechenden Information oder Erfahrung konfrontiert sind (z. B. *Links, die sie zu den einschlägigen Teilen der Datenschutzerklärung weiterleiten*).

Kontakt Daten: Die Kontaktadresse des Unternehmens, an die Datenschutzanfragen gerichtet werden können, sollte in der Datenschutzerklärung deutlich angegeben werden. Sie sollte in einem Abschnitt erscheinen, in dem die Nutzer:innen diese Angabe erwarten können, beispielsweise in einem Abschnitt über die Identität des Verantwortlichen, in einem rechtebezogenen Abschnitt oder in einem Abschnitt mit Kontaktdaten.

Erreichbarkeit der Aufsichtsbehörde: Angabe der genauen Bezeichnung der Aufsichtsbehörde und eines Links zu ihrer Website oder der dortigen speziellen Seite, auf der eine Beschwerde eingereicht werden kann. Diese Informationen sollten in einem Abschnitt erscheinen, in dem die Nutzer:innen sie erwarten können, beispielsweise in einem Abschnitt, der sich auf Rechte bezieht.

Überblick über die Datenschutzerklärung: Am Anfang/im Kopfteil der Datenschutzerklärung sollten Sie ein (ausblendbares) Inhaltsverzeichnis mit Überschriften und Unterüberschriften bereitstellen, aus dem die verschiedenen Passagen der Datenschutzhinweise ersichtlich sind. Die Namen der einzelnen Passagen führen die Nutzer:innen eindeutig zu den genauen Inhalten und ermöglichen es ihnen, den gesuchten Abschnitt schnell zu ermitteln und zu erreichen.

Änderungshistorien und Vergleich: Werden am Datenschutzhinweis Änderungen vorgenommen, machen Sie frühere Versionen mit dem Datum der Veröffentlichung zugänglich und heben Sie Änderungen hervor.

Einheitliche Formulierungen: Auf der Website werden für dieselben Datenschutzbestimmungen jeweils dieselben Formulierungen und Begriffsbestimmungen verwendet. Die in der Datenschutzerklärung verwendete Formulierung sollte derjenigen entsprechen, die auf der übrigen Plattform verwendet wird.

Begriffsbestimmungen bereitstellen: Werden ungewohnte oder fachspezifische Wörter oder Jargons verwendet, hilft die Bereitstellung einer Begriffsbestimmung in einfacher Sprache den Nutzer:innen beim Verständnis der Informationen, die ihnen zur Verfügung gestellt werden. Die Begriffsbestimmung kann direkt im Text erfolgen, wenn Nutzer:innen mit dem Mauszeiger über das betreffende Wort fahren, oder in einem Glossar zur Verfügung gestellt werden.

Hervorgehobene Datenschutzelemente: Elemente oder Handlungen mit Bezug zum Datenschutz werden auf einer Benutzeroberfläche, die dem betreffenden Thema nicht unmittelbar gewidmet ist, visuell auffällig dargestellt. Wenn beispielsweise auf der Plattform eine öffentliche Nachricht gepostet wird, sollten Steuerungsmöglichkeiten für die Verknüpfung des geografischen Standorts direkt verfügbar und deutlich sichtbar sein.

Einführung in den Datenschutz (Onboarding): Social-Media-Anbieter sollten im Rahmen des Anmeldeprozesses unmittelbar nach der Einrichtung eines Kontos Aspekte zum Datenschutz aufnehmen, damit die Nutzer:innen ihre Präferenzen problemlos entdecken und festlegen können. Dies kann beispielsweise dadurch geschehen, dass sie aufgefordert werden, ihre Datenschutzpräferenzen festzulegen, nachdem sie ihren ersten Freund hinzugefügt oder ihren ersten Post geteilt haben.

Verwendung von Beispielen: Neben obligatorischen Angaben, die den Zweck der Verarbeitung klar und präzise angeben, können Beispiele verwendet werden, um eine bestimmte Datenverarbeitung zu veranschaulichen, sodass sie für die Nutzer:innen konkreter und besser greifbar wird.

Kontextbezogene Informationen: Zusätzlich zu einer umfassenden Datenschutzerklärung sollten zu dem für den Nutzer:innen am besten geeigneten Zeitpunkt kurze Informationen zur Verfügung gestellt werden, damit dieser spezifische, kontinuierliche Informationen über die Art und Weise erhält, wie seine Daten verarbeitet werden.

3.2 In den sozialen Medien auf dem Laufenden bleiben

Anwendungsfall 2a: Mehrschichtige Datenschutzhinweise

a. Beschreibung des Kontextes

66. Wie bereits in den Leitlinien für Transparenz hervorgehoben wurde, ist der Grundsatz der Transparenz eng mit dem Grundsatz der Verarbeitung personenbezogener Daten nach Treu und Glauben verknüpft.⁴⁰ Informationen über die Verarbeitung personenbezogener Daten führen dazu, dass die Verantwortlichen ihre eigenen Handlungen reflektieren, dass die Datenverarbeitung für die betroffenen Personen verständlicher wird und letztlich die betroffenen Personen in die Lage versetzt werden, insbesondere durch die Ausübung ihrer Rechte Kontrolle über ihre Daten zu haben. Die daraus resultierende Angleichung der Fähigkeiten der beteiligten Personen führt zu einem auf Treu und Glauben basierenden System der Verarbeitung personenbezogener Daten. Mehr Informationen bedeuten jedoch nicht unbedingt bessere Informationen. Ein Übermaß an irrelevanten oder verwirrenden Informationen kann wichtige inhaltliche Aspekte verschleiern oder die Wahrscheinlichkeit, sie zu finden, verringern. Daher ist das richtige Gleichgewicht zwischen Inhalt und verständlicher Darstellung in diesem Bereich von entscheidender Bedeutung. Wird dieses Gleichgewicht nicht erreicht, kann es zu irreführenden Gestaltungsmustern kommen.

b. Maßgebliche Rechtsvorschriften

67. Die soeben skizzierten Verknüpfungen werden auf der Grundlage von Artikel 5 DS-GVO deutlich. Transparenz und Verarbeitung nach Treu und Glauben werden in Artikel 5 Absatz 1 Buchstabe a DS-GVO bereits systematisch nebeneinander erwähnt, da eine Komponente die andere bestimmt. Die Tatsache, dass nicht nur externe, sondern auch interne Transparenz bestehen muss, wird auch durch die Rechenschaftspflicht in Artikel 5 Absatz 2 DS-GVO verdeutlicht. Der wichtigste Teil der internen Transparenz ist die Anforderung, gemäß Artikel 30 DS-GVO ein Verzeichnis von Verarbeitungstätigkeiten zu führen. Hinsichtlich der externen Transparenz können Social-Media-Anbieter den Nutzer:innen neben anderen Informationsmitteln Mehrebenen-Datenschutzhinweise zur Verfügung stellen.⁴¹ Diese Notwendigkeit der Verständlichkeit und der Verarbeitung nach Treu und Glauben schlägt sich ferner in den Anforderungen des Artikels 12 Absatz 1 DS-GVO nieder, wonach alle in den Artikeln 13 und 14 DS-GVO genannten Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln sind. Folglich muss der Informationsinhalt hindernisfrei zur Verfügung gestellt werden. Sind die Voraussetzungen des Artikels 12 DS-GVO nicht erfüllt, liegen keine gültigen Informationen im Sinne der Artikel 13 und 14 DS-GVO vor. Somit können, im Sinne einer wirksamen Kontrolle, Verantwortliche und Auftragsverarbeiter zur Rechenschaft gezogen werden, was dazu führt, dass die Anforderungen der DS-GVO in der Praxis wirkungsvoll sind.

⁴⁰ Leitlinien für Transparenz, S. 4-5.

⁴¹ Siehe Anwendungsfall 2.a in Abschnitt 3.2.

c. Irreführende Gestaltungsmuster

i. Inhaltsbezogene Muster

68. In Bezug auf diesen Anwendungsfall finden inhaltsbezogene Muster ihre Grenzen in Artikel 12 Absatz 1 DS-GVO, der in Bezug auf die übermittelten Informationen eine präzise und verständliche Form sowie eine klare und einfache Sprache vorschreibt.

Im Dunkeln gelassen – Widersprüchliche Informationen (Anhang I Checkliste 4.6.2)

69. Einer der offensichtlichsten Fälle, in denen dies eintreten kann, ist die Übermittlung **widersprüchlicher Informationen**, welche die Nutzer:innen im Ungewissen darüber lassen, was sie tun sollten und was die Folgen ihrer Handlungen wären, sodass sie keine Einstellungen vornehmen oder die Standardeinstellungen beibehalten.
70. Verstöße in diesem Bereich, wie der Verstoß gegen Artikel 12 Absatz 1 DS-GVO, können durch andere Effekte wie **Emotionale Steuerung** verstärkt werden. Motivierende Texte, Bilder und Farben sowie ansprechende Werbung sind grundsätzlich zulässig. Sie dürften jedoch die Wirkung irreführender Gestaltungsmuster, einschließlich gegen Treu und Glauben verstoßende Verarbeitungen im Sinne von Artikel 5 Absatz 1 Buchstabe a DS-GVO, verstärken.

Sharing your information

On our platform you can **share everything and anything!** The more you share, the **more exciting** your **experience** will be! And at any time you can set your preference on the visibility of the information you share on our platform.

For example, you can decide if you want to **share your geolocation** or who will be able to read your posts.

If you **change the publicity of your information** once it is posted online, you will lose visibility and some people might not be able to see it anymore.



Beispiel 12: In diesem Beispiel zeichnen die Informationen im Zusammenhang mit der Weitergabe von Daten ein äußerst positives Bild der Verarbeitung, indem sie die Vorteile des Austauschs möglichst vieler Daten hervorheben. In Verbindung mit der Abbildung, die das Foto eines niedlichen, mit einem Ball spielenden Tieres darstellt, kann diese **Emotionale Steuerung** Nutzer:innen im Hinblick auf die potenziellen Risiken der Weitergabe von Informationen auf der Plattform die Illusion der Sicherheit und Geborgenheit vermitteln. Auf der anderen Seite sind Informationen darüber, wie man die Öffentlichkeit der eigenen Daten kontrolliert, unklar. Zunächst heißt es, dass die Nutzer:innen ihre Präferenz hinsichtlich der Weitergabe von Daten jederzeit festlegen können. Dann jedoch geht aus dem letzten Satz hervor, dass dies nicht möglich ist, wenn auf der Plattform bereits etwas veröffentlicht wurde. Diese **widersprüchlichen Informationen** lassen Nutzer:innen im Ungewissen darüber, wie sie die Öffentlichkeit ihrer Daten kontrollieren können.

Unbeständig – Fehlende Hierarchie (Anhang I Checkliste 4.5.1)

71. Ähnliche Auswirkungen wie bei **widersprüchlichen Informationen** und **emotionaler Steuerung** können vorkommen, wenn die Darstellung der Informationen weder einem internen System noch einer Hierarchie folgt. **Fehlende Hierarchie** der Datenschutzinformationen liegt vor, wenn diese Informationen mehrfach erscheinen und auf unterschiedliche Weise dargestellt werden. Nutzer:innen dürften durch diese Wiederholungen verwirrt werden und anschließend nicht in der Lage sein, zu verstehen, wie ihre Daten verarbeitet werden und wie sie Kontrolle über diese ausüben können. Eine solche Gestaltung erschwert das Verständnis von Informationen, da das vollständige Bild nicht leicht zugänglich ist. In Fällen wie dem im folgenden Beispiel beschriebenen verstößt dies gegen die Anforderungen an Verständlichkeit und leichte Zugänglichkeit nach Artikel 12 Absatz 1 DS-GVO.

Beispiel 13: Informationen über die Rechte betroffener Personen sind über die gesamten Datenschutzhinweise verteilt. Obwohl im Abschnitt „Ihre Optionen“ verschiedene Rechte betroffener Personen erläutert werden, erscheinen Informationen über das Recht, Beschwerde einzulegen, und die genaue Kontaktadresse erst nach mehreren Abschnitten und Ebenen, die sich auf andere Themen beziehen. In den Datenschutzhinweisen werden somit Kontaktdaten an Stellen teilweise weggelassen, an denen sie wünschenswert und ratsam wären.

72. **Fehlende Hierarchie** kann auch vorliegen, wenn die übermittelten Informationen so strukturiert sind, dass den Nutzer:innen die Orientierung erschwert wird, wie im folgenden Beispiel gezeigt wird.

Beispiel 14: Die Datenschutzerklärung ist nicht in verschiedene Abschnitte mit Titeln und Inhalten unterteilt. Es werden mehr als 70 Seiten bereitgestellt. Es gibt aber weder seitlich noch oben in der Erklärung ein Navigationsmenü, das den Nutzer:innen den einfachen Zugang zu dem gesuchten Abschnitt erlaubt. Die Erläuterung des selbst geschaffenen Begriffs „Entstehungsdaten“ ist in einer Fußnote auf Seite 67 enthalten.

Im Dunkeln gelassen – Mehrdeutige Formulierungen oder Informationen (Anhang I Checkliste 4.6.3)

73. Auch wenn die Wortwahl nicht offenkundig widersprüchlich ist, kann die Verwendung von mehrdeutigen und vagen Begriffen bei der Information von Nutzer:innen zu Problemen führen. Mit solchen Informationen werden die Nutzer:innen wahrscheinlich im Ungewissen darüber gelassen, wie die Daten verarbeitet werden oder wie sie eine gewisse Kontrolle über die Daten ausüben können. Wenn davon ausgegangen werden kann, dass durchschnittliche Nutzer:innen die tatsächliche Aussage der Informationen ohne besondere Kenntnisse wahrscheinlich nicht verstehen, sind die Voraussetzungen des Artikels 12 Absatz 1 DS-GVO nicht erfüllt. Im weiteren Sinne kann die Verwendung **mehrdeutiger Formulierungen oder Informationen** im Widerspruch zum Grundsatz der Verarbeitung nach Treu und Glauben des Artikels 5 Absatz 1 Buchstabe a DS-GVO stehen, da die Informationen nicht als transparent angesehen werden können und den betroffenen Personen die Möglichkeit genommen wird, die Verarbeitung ihrer personenbezogenen Daten zu verstehen und ihre Rechte auszuüben.

Beispiel 15: Datenschutzhinweise beschreiben einen Teil einer Verarbeitung vage und ungenau, wie in diesem Satz: „Ihre Daten könnten zur Verbesserung unserer Dienste verwendet werden“. Darüber hinaus gilt das Recht auf Auskunft über personenbezogene Daten gemäß Artikel 15 Absatz 1 DS-GVO für die Verarbeitung; dieses wird jedoch in einer Weise erwähnt, aus der den Nutzer:innen nicht klar

wird, worauf sie zugreifen dürfen: „Sie können einen Teil Ihrer Informationen in Ihrem Konto einsehen und dadurch, dass Sie überprüfen, was Sie auf der Plattform veröffentlicht haben“.

74. Im Beispiel lässt die Verwendung der Bedingungsform („könnten“) die Nutzer:innen im Ungewissen, ob man ihre Daten zur Verarbeitung nutzen wird oder nicht. Der Begriff „Dienste“ erscheint zu allgemein, um als „klar“ eingestuft zu werden. Darüber hinaus ist unklar, wie man die Daten zur Verbesserung der Dienste verarbeiten wird. Der EDSA weist darauf hin, dass die Verwendung der Bedingungsform oder vager Formulierungen keine „klare und einfache Sprache“ im Sinne von Artikel 12 Absatz 1 Satz 1 DS-GVO darstellt und nur eingesetzt werden darf, wenn die Verantwortlichen nachweisen können, dass dies den Grundsatz von Treu und Glauben bei der Verarbeitung nicht aushöhlt.⁴²

Unbeständig – Sprachliche Diskontinuität (Anhang I Checkliste 4.5.4)

75. Werden den Einwohnern bestimmter Mitgliedstaaten Online-Dienste angeboten und an sie gerichtet, sollten die Datenschutzhinweise auch in diesen Sprachen angeboten werden.⁴³ In diesem Zusammenhang ist es wichtig, dass bei der Wahl einer bestimmten Sprache auch manuell umgeschaltet werden kann und dass dies kontinuierlich, ohne Unterbrechungen umgesetzt wird. Werden diese Kriterien nicht erfüllt, sind die betroffenen Personen mit einer **sprachlichen Diskontinuität** konfrontiert, mit der Folge, dass sie nicht in der Lage sind, Informationen über den Datenschutz zu verstehen. Nutzer:innen werden mit diesem irreführenden Gestaltungsmuster konfrontiert, wenn Datenschutzinformationen nicht in den Amtssprachen des Landes, in dem sie leben, übermittelt werden, während der Dienst in dieser Sprache bereitgestellt wird. Beherrschen Nutzer:innen die Sprache nicht, in der die Datenschutzinformationen bereitgestellt werden, können sie diese nicht problemlos lesen und wissen daher nicht, wie ihre personenbezogenen Daten verarbeitet werden. Hier ist zu beachten, dass **sprachliche Diskontinuität** Nutzer:innen verwirren und eine Umgebung für die Einstellungen schaffen kann, von der sie nicht wissen, wie sie sie nutzen sollen. Dieses irreführende Gestaltungsmuster kann, wie in diesen Leitlinien durchgängig gezeigt wird, auf unterschiedliche Weise auftreten.

Beispiel 16:

Variante A: Die Social-Media-Plattform steht auf Kroatisch als von den Nutzer:innen gewählte Sprache (oder auf Spanisch als Sprache des Landes, in dem sie sich befinden) zur Verfügung, während alle oder bestimmte Informationen zum Datenschutz nur auf Englisch verfügbar sind.

Variante B: Jedes Mal, wenn Nutzer:innen bestimmte Seiten (z. B. die Hilfeseite) aufrufen, wechseln diese automatisch in die Sprache des Landes, in dem sie sich befinden, selbst wenn sie zuvor eine andere Sprache gewählt haben.

76. Variante A veranschaulicht den Fall, dass keine Informationen in einer von der betroffenen Person offenbar beherrschten Sprache verfügbar sind. Dies bedeutet, dass sie die Informationen nicht lesen und somit nicht verstehen kann, wie ihre personenbezogenen Daten verarbeitet werden. Die Informationen können nicht als verständlich im Sinne der Vorschriften in Artikel 12 Absatz 1 DS-GVO

⁴² Siehe Leitlinien für Transparenz, Rn. 12, einschließlich der „Beispiele für ungenügende Verfahren“, und Rn. 13.

⁴³ Siehe Leitlinien für Transparenz, Rn. 13 und Fußnote 15.

angesehen werden. Aufgrund des Fehlens von Datenschutzinformationen in der Sprache, die verstanden wird, kann nicht davon ausgegangen werden, dass den betroffenen Personen die nach Artikel 13 bzw. 14 DS-GVO erforderlichen Informationen übermittelt wurden.

77. Variante B beschreibt einen Fall, in dem Informationsseiten zum Datenschutz standardmäßig in der Sprache des Wohnsitzlandes des Nutzers erscheinen, obwohl eine klare Sprachauswahl vorgenommen wurde. Dies bedeutet, dass Nutzer:innen jedes Mal, wenn sie auf eine Seite mit Datenschutzinformationen zugreifen, ihre Sprachpräferenz zurücksetzen müssen. Dies kann als unlautere Praxis gegenüber betroffenen Personen betrachtet werden und könnte einen Verstoß gegen den in Artikel 5 Absatz 1 Buchstabe a DS-GVO verankerten Grundsatz der Verarbeitung nach Treu und Glauben bedeuten.

ii. Oberflächenbezogene Muster

78. Mitunter nutzen Social-Media-Anbieter spezielle Verfahren für die Darstellung ihrer Datenschutzeinstellungen. Während des Anmeldeverfahrens werden Nutzer:innen zahlreiche Informationen und unterschiedliche Einstellungen zum Datenschutz übermittelt. Um sicherzustellen, dass die Nutzer:innen bei der Nutzung der Plattform jederzeit den Weg zu diesen Einstellungen finden und Änderungen vornehmen können, sollten die Einstellungen leicht zugänglich und mit einschlägigen Informationen verknüpft sein, damit die Nutzer:innen eine Entscheidung in informierter Weise treffen können. Das Element „leicht zugänglich“ bedeutet, dass betroffene Personen die Informationen nicht erst suchen müssen. Was die Datenschutzerklärungen betrifft, so hat die Artikel-29-Datenschutzgruppe bereits erklärt, dass Anordnungs- oder Farbsysteme, die einen Text oder Link schlechter erkennbar oder auf einer Website schwer auffindbar machen, nicht als leicht zugänglich erachtet werden.⁴⁴

Überfrachtung – Datenschutz-Labyrinth (Anhang I Checkliste 4.1.2)

79. Nach den Leitlinien für Transparenz sollten die Datenschutzhinweise leicht zugänglich sein, d. h. durch einen einzigen Klick auf Websites.⁴⁵ Die Verwendung eines Mehrebenen-Ansatzes kann dazu beitragen, die Datenschutzhinweise im Sinne von Artikel 12 Absatz 1 DS-GVO deutlicher darzustellen.⁴⁶ Dies sollte jedoch nicht zur Folge haben, dass die Ausübung wichtiger Funktionen oder Rechte unnötig erschwert wird, indem eine komplexe Datenschutzerklärung mit unzähligen Ebenen eingeführt wird, die zu dem irreführenden Gestaltungsmuster ***Datenschutz-Labyrinth*** führen würde. Dieses Muster entspricht einer Situation, in der Informationen über den Datenschutz oder Kontrollfunktionen für den Datenschutz besonders schwer zu finden sind, weil Nutzer:innen durch zahlreiche Seiten navigieren müssen, ohne eine umfassende, vollständige Übersicht zu erhalten. Dies führt wahrscheinlich dazu, dass die Nutzer:innen die maßgeblichen Informationen/Einstellungen übersehen oder die Suche aufgeben. Die mehrere Ebenen umfassende Anordnung dient dazu, die Lesbarkeit zu erleichtern und Informationen darüber zu liefern, wie die betroffenen Personen ihre Rechte wahrnehmen können, nicht dazu, dies zu erschweren. Es ist von wesentlicher Bedeutung, dafür zu sorgen, dass Nutzer:innen den Erläuterungen leicht folgen können.

⁴⁴ Leitlinien für Transparenz, Rn. 11.

⁴⁵ Siehe Leitlinien für Transparenz, Beispiel in Rn. 11.

⁴⁶ Einzelheiten zum Mehrebenen-Ansatz in einem digitalen Umfeld finden sich in den Leitlinien für Transparenz, Rn. 35-37.

80. In dieser Hinsicht ist die beste Option für Nutzer:innen nicht eine Herangehensweise „von der Stange“; sie hängt vielmehr von vielen Kriterien wie beispielsweise der Art der Nutzer:innen auf der Plattform oder der allgemeinen Art der Gestaltung der App ab. Nach Möglichkeit sollte die implementierte Mehrebenen-Lösung mit Nutzer:innen getestet werden, um ihre Rückmeldungen einzuholen und die Wirksamkeit der Lösung zu bewerten. Aus diesem Grund kann für die maximal zulässige Anzahl von Informationsebenen keine konkrete Zahl festgelegt werden. Es muss daher stets durch eine Einzelfallprüfung ermittelt werden, ob zu viele Ebenen eingesetzt werden und es somit zu irreführenden Gestaltungsmustern kommt. Je höher die Zahl der Ebenen, desto wahrscheinlicher ist es, dass Nutzer:innen abgeschreckt oder irregeführt werden. Eine hohe Anzahl von Ebenen wird nur für Sonderfälle geeignet sein, in denen eine umfassende Bereitstellung der komplexen Informationen nicht einfach ist. Zugleich darf der Mehrebenen-Ansatz nicht dazu missbraucht werden, Informationen in tieferen Ebenen zu verbergen oder unnötige Ebenen hinzuzufügen.
81. Dies ist jedoch anders zu beurteilen, wenn es um die Ausübung von Nutzerrechten geht. Die DS-GVO schreibt vor, die Ausübung dieser Rechte stets zu gewährleisten. Dieser Rahmen regelt die Darstellung von Informationen über verbundene Funktionen und die Ausübung von Rechten. Wenn Nutzer:innen ihre Rechte ausüben wollen, sollte die Zahl der Schritte so gering wie möglich sein. Daher sollten Nutzer:innen möglichst auf direktem Wege zu der Funktion gelangen, die ihnen die Ausübung ihrer Rechte ermöglicht. In den meisten Fällen könnten Nutzer:innen von der Ausübung dieser Rechte abgehalten werden, wenn sie durch eine große Zahl von Informationsebenen navigieren müssen, bevor sie mit Hilfe von Funktionen ihre Rechte tatsächlich ausüben können. Wird eine hohe Zahl von Schritten implementiert, sollte der Social-Media-Anbieter in der Lage sein, die Vorteile für die Nutzer:innen als betroffene Personen gemäß der DS-GVO nachzuweisen. Neben der Erläuterung der Rechte betroffener Personen in den Datenschutzhinweisen gemäß den Anforderungen in Artikel 13 Absatz 2 Buchstaben b, c und d DS-GVO sollte die Ausübung der Rechte auch unabhängig von diesen Informationen zugänglich sein. Nutzer:innen sollten beispielsweise die Möglichkeit haben, ihre Rechte als betroffene Personen auch über das Menü der Plattform auszuüben.

Beispiel 17: Auf seiner Plattform stellt der Social-Media-Anbieter ein Dokument mit der Bezeichnung „*Hilfreiche Hinweise*“ zur Verfügung, das auch wichtige Informationen über die Ausübung der Rechte betroffener Personen enthält. Die Datenschutzerklärung enthält jedoch keinen Link oder sonstige Hinweise zu diesem Dokument. Stattdessen wird dort erwähnt, dass weitere Einzelheiten im Abschnitt „Fragen und Antworten“ der Website zu finden sind. Nutzer:innen, die in der Datenschutzerklärung Informationen über ihre Rechte erwarten, werden folglich diese Erläuterungen dort nicht finden; sie müssen weiter navigieren und den Abschnitt „Fragen und Antworten“ danach durchsuchen.

82. Dieses Beispiel zeigt eindeutig ein Muster des Typs **Datenschutz-Labyrinth**, das entgegen Artikel 12 Absatz 2 DS-GVO den Zugang zu weiteren Informationen über die Rechte betroffener Personen und insbesondere das Auffinden von Informationen über die Art und Weise, wie diese Rechte ausgeübt werden können, erschwert. Ist die Datenschutzerklärung unvollständig, verstößt dies darüber hinaus auch gegen Artikel 13 Absatz 2 Buchstaben b, c und d bzw. Artikel 14 Absatz 2 Buchstaben c, d und e DS-GVO. Während ausführlichere Informationen oder das direkte Mittel zur Ausübung der Rechte nur einen Klick von der Stelle, an der sie in der Datenschutzerklärung genannt werden, entfernt sein könnten, müssen die Nutzer:innen in diesem Beispiel zum Abschnitt „Fragen und Antworten“ navigieren und ihn durchsuchen, um das Dokument „*Hilfreiche Hinweise*“ zu finden.

83. Es sollte beachtet werden, dass es sogar zu noch stärkeren Effekten als denen durch zu viele Ebenen⁴⁷ kommen kann, wenn nicht nur mehrere Geräte, sondern auch mehrere, von derselben Social-Media-Plattform bereitgestellte Apps wie beispielsweise besondere Messenger-Apps genutzt werden. Nutzer:innen, die diese Art von sekundärer App nutzen, ständen größeren Hindernissen und Mühen gegenüber, wenn sie die Browserversion oder die primäre App aufrufen müssten, um datenschutzbezogene Informationen zu erhalten. In einer solchen Situation, die nicht nur geräteübergreifend, sondern auch App-übergreifend ist, müssen die einschlägigen Informationen stets unmittelbar zugänglich sein, unabhängig davon, auf welche Weise die Nutzer:innen die Plattform verwenden.

Behindern – Sackgasse (Anhang I Checkliste 4.4.1)

84. Verstöße gegen rechtliche Anforderungen können auch dann vorliegen, wenn die nach der DS-GVO erforderlichen Datenschutzinformationen durch weitere Maßnahmen wie Klicken auf einen Link oder eine Schaltfläche zur Verfügung gestellt werden. Insbesondere können eine fehlgeleitete Navigation oder eine uneinheitliche Gestaltung der Benutzeroberfläche, die wirkungslose Funktionen nach sich ziehen, nicht als dem Grundsatz von Treu und Glauben nach Artikel 5 Absatz 1 Buchstabe a DS-GVO entsprechend eingestuft werden, denn Nutzer:innen werden irregeführt, wenn sie entweder versuchen, Zugang zu bestimmten Informationen zu erhalten oder ihre Datenschutzpräferenzen festzulegen. **Sackgassen**, in denen Nutzer:innen ohne Funktionen zur Wahrnehmung ihrer Rechte sich selbst überlassen werden, sollten daher auf jeden Fall vermieden werden; sie verstoßen unmittelbar gegen Artikel 12 Absatz 2 DS-GVO, wonach der Verantwortliche die Ausübung von Rechten erleichtern muss.

Beispiel 18: Ein Social-Media-Anbieter bietet in seiner Datenschutzerklärung zahlreiche Hyperlinks zu Seiten mit weiteren Informationen zu bestimmten Themen an. In der Datenschutzerklärung gibt es jedoch mehrere Teile, die nur allgemeine Aussagen darüber enthalten, dass es möglich sei, auf weitere Informationen zuzugreifen, ohne anzugeben, wo und wie.

85. Die Datenschutzerklärung wird im Allgemeinen als das Dokument angesehen, in dem alle Informationen über Aspekte des Datenschutzes im Einklang mit den in den Artikeln 12, 13 und 14 DS-GVO festgelegten Verpflichtungen zentral zusammengeführt werden. Daher muss auch dafür gesorgt werden, dass die Nutzer:innen an alle relevanten Stellen auf der Social-Media-Plattform weitergeleitet werden, damit sie ihre Daten kontrollieren oder ihre Rechte ausüben können. In Beispiel 18 wird dies nur teilweise umgesetzt, da für einige Elemente Links zu weiteren Informationen bereitgestellt werden, für andere aber nicht. Bei diesen Elementen kann das Gestaltungsmuster **Sackgasse** zu einem Verstoß gegen Artikel 12 Absatz 1 DS-GVO führen, indem der Zugang zu bestimmten Datenschutzinformationen erschwert wird, oder es führt zu einem Verstoß gegen Artikel 12 Absatz 2 DS-GVO, da die Ausübung der Rechte nicht erleichtert wird.

d. Best Practices

Angeheftete Navigationsleiste: Beim Lesen einer Seite zum Datenschutz kann das Inhaltsverzeichnis ständig auf dem Bildschirm angezeigt werden, sodass sich die Nutzer:innen stets auf der Seite verorten und dank Verlinkungen schnell im Inhalt navigieren können.

⁴⁷ Siehe Rn. 81 und 82.

Zurück zum Seitenanfang: Fügen Sie am unteren Ende der Seite oder als angeheftetes Element am unteren Ende des Fensters eine Schaltfläche für die Rückkehr zum Seitenanfang ein, um den Nutzer:innen die Navigation auf einer Seite zu erleichtern.

Schnellzugriffe: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 29). *(Stellen Sie beispielsweise in der Datenschutzerklärung für jede Datenschutzinformation einen Link bereit, der direkt zu den entsprechenden Datenschutzseiten auf der Social-Media-Plattform weiterleitet).*

Kontaktdaten: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 29).

Erreichbarkeit der Aufsichtsbehörde: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 29).

Überblick über die Datenschutzerklärung: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 29).

Änderungshistorien und Vergleich: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 29).

Einheitliche Formulierungen: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 29).

Begriffsbestimmungen bereitstellen: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 29).

Verwendung von Beispielen: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 30).

Anwendungsfall 2b: Unterrichtung der betroffenen Person über gemeinsame Verantwortlichkeit, Artikel 26 Absatz 2 DS-GVO

a. Beschreibung des Kontextes und maßgebliche Rechtsvorschriften

86. Artikel 26 Absatz 2 Satz 2 DS-GVO enthält zusätzliche Transparenzbestimmungen für den besonderen Fall der gemeinsamen Verantwortlichkeit.⁴⁸ Dadurch wird sichergestellt, dass den betroffenen Personen das Wesentliche der Vereinbarung über die gemeinsame Verantwortlichkeit bekannt ist.⁴⁹ In seinen Leitlinien 7/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DS-GVO empfiehlt der EDSA, dass das Wesentliche zumindest alle Elemente der in den Artikeln 13 und 14 der DS-GVO genannten Informationen umfasst, die den betroffenen Personen bereits zugänglich sein sollten, und dass für jedes Element festgelegt werden sollte, welcher der gemeinsam Verantwortlichen für die Gewährleistung der Einhaltung verantwortlich ist.⁵⁰ Das Wesentliche der Vereinbarung muss auch die Anlaufstelle umfassen, falls eine solche benannt wurde. Es ist Sache der gemeinsam Verantwortlichen, zu entscheiden, wie das Wesentliche der Vereinbarung den betroffenen Personen am wirksamsten zur Verfügung gestellt werden kann.⁵¹

b. Irreführende Gestaltungsmuster

⁴⁸ Zur Definition des Begriffs „gemeinsame Verantwortlichkeit“ siehe Artikel 4 Nummer 7 in Verbindung mit Artikel 26 Absatz 1 Satz 1 DS-GVO sowie die EDSA-Leitlinien 7/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DS-GVO, angenommen am 7. Juli 2021, Version 2.1, Rn. 46-49, abrufbar unter: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_de.pdf.

⁴⁹ Siehe EDSA-Leitlinien 7/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“, Rn. 179.

⁵⁰ Siehe EDSA-Leitlinien 7/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“, Rn. 180, auch bezüglich des nächsten Satzes.

⁵¹ EDSA-Leitlinien 7/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“, Rn. 181.

Beispiel 19: Hinsichtlich irreführender Gestaltungsmuster besteht die Herausforderung für die Verantwortlichen in dieser Konstellation darin, diese Informationen so in das Online-System zu integrieren, dass sie leicht erkennbar sind und ihre Klarheit und Verständlichkeit nicht verlieren, auch wenn Artikel 12 Absatz 1 Satz 1 DS-GVO nicht unmittelbar auf Artikel 26 Absatz 2 Satz 2 DS-GVO verweist. Aufgrund der Datenschutzgrundsätze der Verarbeitung nach Treu und Glauben, Transparenz und Rechenschaftspflicht nach Artikel 5 Absatz 1 Buchstabe a und Absatz 2 DS-GVO ergeben sich jedoch auch im Fall der gemeinsamen Verantwortlichkeit vergleichbare Anforderungen. Wenn gemeinsam Verantwortliche Informationen über das Wesentliche der Vereinbarung in den Datenschutzhinweisen bereitstellen, muss dies ebenfalls in klarer und transparenter Weise geschehen. Daher kann die Verarbeitung nicht mehr als dem Grundsatz von Treu und Glauben entsprechend bewertet werden, wenn die Informationen darüber schwer zu erfassen sind, da keine Links bereitgestellt werden oder die Informationen über mehrere Informationsbereiche verteilt sind. Das irreführende Gestaltungsmuster ***Datenschutz-Labyrinth***⁵² könnte noch verwirrender sein, als dies im Allgemeinen in Datenschutzhinweisen der Fall sein kann, da die Nutzer:innen erwarten können, dass die Informationen nach Artikel 26 Absatz 2 Satz 2 DS-GVO lückenlos gegeben werden. Ein Social-Media-Anbieter bezieht sich im Rahmen der Datenschutzerklärung stets auf „Entstehungsdaten“ und benutzt nicht den Begriff personenbezogene Daten. Nur auf Seite 90 enthält der Mehrebenen-Datenschutzhinweis die Erläuterung, dass „Entstehungsdaten personenbezogene Daten der Nutzer:innen umfassen könnten“. Die den betroffenen Personen zur Verfügung gestellte Darstellung der wesentlichen Aspekte der Vereinbarung der gemeinsam Verantwortlichen verwendet ebenfalls den Begriff „Entstehungsdaten“, ohne ihn zu erläutern. Der andere gemeinsam Verantwortliche (B) definiert den Begriff „personenbezogene Daten“ in seiner eigenen Datenschutzerklärung. In seinem dem Datenschutz gewidmeten Abschnitt über die gemeinsame Verantwortlichkeit mit dem Social-Media-Anbieter gibt B jedoch nur einen Link zu der von dem Anbieter bereitgestellten Vereinbarung an, ohne dass eine weitere Erläuterung erfolgt.

87. Die Erläuterungen nach Artikel 26 Absatz 2 Satz 2 DS-GVO sind schwieriger zu verstehen, wenn sie nicht mehr einheitlich sind. Diese Uneinheitlichkeit wird verstärkt, wenn Social-Media-Plattformen eine selbst-kreierte Terminologie verwenden, die die Nutzer:innen in der Regel nicht mit der Verarbeitung personenbezogener Daten in Verbindung bringen, wie in Beispiel 19 gezeigt wird. In dem Beispiel verstoßen beide gemeinsam Verantwortlichen gegen Artikel 26 Absatz 2 Satz 2 DS-GVO sowie gegen Artikel 5 Absatz 1 Buchstabe a DS-GVO, da die Informationen über die gemeinsame Verantwortlichkeit unklar und daher für die betroffenen Personen nicht transparent sind.

Anwendungsfall 2c: Benachrichtigung der betroffenen Person im Falle einer Verletzung des Schutzes personenbezogener Daten (sogenannte ‚Datenpanne‘)

a. Beschreibung des Kontextes und maßgebliche Rechtsvorschriften

⁵² Siehe Anwendungsfall 2a, Beispiel 17 in diesen Leitlinien.

88. Um eine Verletzung des Schutzes personenbezogener Daten (im allgemeinen Sprachgebrauch häufig als ‚Datenpanne‘ bezeichnet) erkennen und dagegen vorgehen zu können, muss ein Verantwortlicher in der Lage sein, eine solche zu erkennen.⁵³ Nach Artikel 4 Nummer 12 DS-GVO bedeutet eine „Verletzung des Schutzes personenbezogener Daten“ eine „Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“. Was Verantwortliche bezüglich sozialer Medien betrifft, so kann es auf unterschiedliche Weise zu Datenschutzverletzungen kommen. Ein Beispiel wäre, dass es einem Angreifer gelingt, auf personenbezogene Daten und Chat-Nachrichten der Nutzer:innen zuzugreifen. Alternativ könnte eine App aufgrund eines Programmversagens über die von den Nutzer:innen erteilten Berechtigungen hinaus auf personenbezogene Daten zugreifen. Ein weiteres Beispiel wäre, dass Nutzer:innen Bilder unter der Einstellung „mit meinen besten Freunden teilen“ weitergeben, ihre Bilder aber stattdessen einer größeren Gruppe von Menschen zur Verfügung gestellt werden. Als letztes Beispiel könnte ein Fehler auf einer Social-Media-Plattform mit Echtzeit-Videos weitere Streamings von Inhalten zulassen, obwohl die Nutzer:innen zuvor eine Schaltfläche zum Stoppen der Aufzeichnung gedrückt hatten.
89. Im Falle einer Verletzung des Schutzes personenbezogener Daten unterrichtet der Verantwortliche in jedem Fall die zuständige Aufsichtsbehörde gemäß Artikel 33 DS-GVO, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Hat eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche gemäß Artikel 34 Absätze 1 und 2 DS-GVO die betroffenen Personen im Allgemeinen von der Verletzung. In diesem Fall muss der Verantwortliche die betroffenen Personen unverzüglich informieren. Diese Informationen müssen in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten beschreiben, da Artikel 12 DS-GVO ebenfalls Anwendung findet. Darüber hinaus müssen diese Informationen (siehe auch Artikel 33 Absatz 3 Buchstaben b bis d in Verbindung mit Artikel 34 Absatz 2 DS-GVO) zumindest Angaben und Maßnahmen wie die Folgenden enthalten:
- gegebenenfalls den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,
 - eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten und
 - eine Beschreibung der vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung, gegebenenfalls einschließlich der Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.⁵⁴
90. Solche Benachrichtigungen von Datenschutzverletzungen nach Artikel 34 DS-GVO können ebenfalls irreführende Gestaltungsmuster enthalten, wenn beispielsweise der jeweilige Verantwortliche den betroffenen Personen alle erforderlichen Informationen zur Verfügung stellt, um sie über den Umfang der Verletzung des Schutzes personenbezogener Daten zu informieren, ihnen aber auch unspezifische und irrelevante Informationen übermittelt neben den Auswirkungen und Vorsichtsmaßnahmen, die

⁵³ Siehe auch EDSA-Leitlinien 1/2021 zu Beispielen für die Meldung von Verletzungen des Schutzes personenbezogener Daten, angenommen am 14. Dezember 2021, Version 2.0, Rn. 4, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_de.

⁵⁴ Vom EDSA gebilligte Leitlinien der Artikel-29-Datenschutzgruppe zur Meldung von Verletzungen des Schutzes personenbezogener Daten, S. 20 <https://ec.europa.eu/newsroom/article29/items/612052/en>.

der Verantwortliche ergriffen hat oder zu ergreifen vorschlägt. Diese teilweise irrelevanten Informationen können irreführend sein und Nutzer:innen, die von dem Verstoß betroffen sind, könnten die Auswirkungen des Verstoßes vielleicht nicht vollständig verstehen oder die (potenziellen) Auswirkungen unterschätzen.

b. Irreführende Gestaltungsmuster

91. Um einige negative Beispiele aufzuzeigen, könnten fehlerhaft umgesetzte Benachrichtigungen von Datenschutzverletzungen, die gegen Artikel 34 DS-GVO in Verbindung mit Artikel 12 DS-GVO verstoßen, folgendermaßen auftreten:

i. Inhaltsbezogene Muster

Im Dunkeln gelassen – Widersprüchliche Informationen (Anhang I Checkliste 4.6.2)

Beispiel 20:

- Der Verantwortliche verweist nur auf Handlungen Dritter und darauf, dass die Verletzung des Schutzes personenbezogener Daten von einem Dritten (z. B. einem Auftragsverarbeiter) verursacht wurde und daher kein Sicherheitsvorfall eingetreten ist. Der Verantwortliche hebt auch einige bewährte Verfahren hervor, die nichts mit dem tatsächlichen Verstoß zu tun haben.
- Der Verantwortliche erklärt die Schwere der Verletzung des Schutzes personenbezogener Daten in Bezug auf sich selbst oder einen Auftragsverarbeiter anstatt in Bezug auf die betroffene Person.

Im Dunkeln gelassen – Mehrdeutige Formulierungen oder Informationen (Anhang I Checkliste 4.6.3)

92. In Bezug auf die in der Benachrichtigung der betroffenen Person über die Verletzung des Datenschutzes benutzte Sprache ist es von entscheidender Bedeutung, dass die Verantwortlichen berücksichtigen, dass die meisten Empfänger nicht mit der besonderen, eventuell fachlichen oder juristischen Sprache im Zusammenhang mit Datenschutz vertraut sind.

Beispiel 21: Aufgrund einer Datenpanne auf einer Social-Media-Plattform hatten unberechtigte Nutzer:innen versehentlich Zugang zu mehreren Sätzen von Gesundheitsdaten. Der Anbieter informierte die Nutzer:innen lediglich darüber, dass „*besondere Kategorien personenbezogener Daten*“ versehentlich öffentlich zugänglich gemacht wurden.

93. Dies stellt eine **mehrdeutige Formulierung** dar, da durchschnittliche Nutzer:innen den Begriff „*besondere Kategorien personenbezogener Daten*“ nicht verstehen und daher nicht wissen, dass ihre Gesundheitsdaten öffentlich gemacht wurden. Dies ist darauf zurückzuführen, dass „*besonders*“ in der allgemeinen Sprache eine ganz andere Bedeutung hat als „*besonders*“ im eng begrenzten Sprachgebrauch der DS-GVO. Durchschnittliche Nutzer:innen wissen nicht, dass nach Artikel 9 Absatz 1 DS-GVO, „*besondere Kategorien personenbezogener Daten*“ personenbezogene Daten umfassen, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen

Person. Somit stellt die Bezeichnung „*besondere Kategorien personenbezogener Daten*“ in diesem Szenario ein irreführendes Gestaltungsmuster dar, da sie die Nutzer:innen täuscht, indem ihr keine weiteren Erläuterungen beigelegt sind Nutzer:innen. Dies ist ein Beispiel für eine Situation, in der ein Verantwortlicher versucht, betroffene Personen über die Verletzung zu informieren, aber seiner Verpflichtung zur Benachrichtigung über die Verletzung des Schutzes personenbezogener Daten gemäß Artikel 34 DS-GVO nicht vollständig nachkommt, da die Schwere des Vorfalls vom durchschnittlichen Leser unterschätzt wird. Die kurzen Informationen im Beispiel sind zudem entgegen der Vorschrift in Artikel 34 in Verbindung mit Artikel 12 Absatz 1 Satz 1 DS-GVO nicht verständlich.

94. Ein weiteres Beispiel für eine **mehrdeutige Formulierung** ist Folgendes:

Beispiel 22: Der Verantwortliche macht bei der Nennung der betroffenen Kategorien personenbezogener Daten nur vage Angaben, indem sich der Verantwortliche z. B. auf von Nutzer:innen übermittelte Dokumente bezieht, ohne anzugeben, welche Kategorien personenbezogener Daten diese Dokumente umfassen und wie sensibel sie waren.

95. Es sollte beachtet werden, dass dieses irreführende Gestaltungsmuster in allen Teilen der Meldung einer Verletzung des Schutzes personenbezogener Daten auftreten kann. Während sich die beiden oben genannten Beispiele auf unklare Formulierungen zu den betroffenen Datenkategorien beziehen, zeigt das nächste Beispiel, dass die Kategorie der von dem Verstoß betroffenen Personen ebenso unklar sein könnte:

Beispiel 23: Bei der Meldung der Verletzung des Schutzes personenbezogener Daten spezifiziert der Verantwortliche die Kategorie der betroffenen Personen nicht hinreichend, indem der Verantwortliche z. B. nur erwähnt, dass betroffene Personen Studierende waren, jedoch nicht angibt, ob es sich bei den betroffenen Personen um Minderjährige oder um schutzbedürftige Personen handelt.

96. Schließlich kann die Schwere des Vorfalls ebenfalls unterschätzt werden, wenn wie im folgenden Beispiel **mehrdeutige Informationen** übermittelt werden:

Beispiel 24: Bei Meldung der Verletzung des Schutzes personenbezogener Daten gegenüber der Aufsichtsbehörde und der betroffenen Person erklärt der Verantwortliche, dass personenbezogene Daten durch andere Quellen veröffentlicht wurden. Die betroffene Person ist daher der Auffassung, dass kein Sicherheitsvorfall vorliegt.

ii. Oberflächenbezogene Muster

97. Auch oberflächenbezogene irreführende Gestaltungsmuster können negative Beispiele für eine Meldung einer Verletzung des Schutzes personenbezogener Daten darstellen, die gegen Artikel 34 DS-GVO in Verbindung mit Artikel 12 DS-GVO verstößt. Dies wird im Folgenden gezeigt:

Überspringen – „Schau, dort drüben“ (Anhang I Checkliste 4.2.2)

Beispiel 25:

- Der Verantwortliche erstattet die Meldung in Form eines Textes, der eine Menge irrelevanter Informationen enthält und die relevanten Einzelheiten übergeht.

- Bei Sicherheitsverletzungen, die sich auf Zugriffsberechtigungen und andere Arten von Daten auswirken, erklärt der Verantwortliche, dass die Daten verschlüsselt oder gehasht sind, während dies nur auf Passwörter zutrifft.

98. Selbst wenn die relevanten Einzelheiten in der Meldung enthalten sind, dürften die betroffenen Personen in diesem Fall durch eine Überfrachtung mit irrelevanten Informationen von ihnen abgelenkt werden.

c. Best Practices

Benachrichtigungen: Benachrichtigungen können verwendet werden, um die Nutzer:innen für Aspekte, Änderungen oder Risiken im Zusammenhang mit der Verarbeitung personenbezogener Daten zu sensibilisieren (z. B. *wenn es zu einer Verletzung des Schutzes personenbezogener Daten kam*). Diese Benachrichtigungen können auf verschiedene Weise umgesetzt werden, beispielsweise durch Nachrichten im Posteingang, Pop-in-Fenster, feste Banner oben auf der Website usw.

Folgen erläutern: Wenn Nutzer:innen eine Datenschutzkontrollfunktion aktivieren oder deaktivieren oder ihre Einwilligung erteilen oder widerrufen wollen, informieren Sie sie auf neutrale Weise über die Folgen einer solchen Handlung.

Schnellzugriffe: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 29) (z. B. *Nutzer:innen einen Link zum Zurücksetzen des Passworts zur Verfügung stellen*).

Einheitliche Formulierungen: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 29).

Begriffsbestimmungen bereitstellen: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 29).

Verwendung von Beispielen: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 30).

3.3 In den sozialen Medien geschützt bleiben

Anwendungsfall 3a: Verwalten der Einwilligung während der Nutzung einer Social-Media-Plattform

a. Beschreibung des Kontextes und maßgebliche Rechtsvorschriften

99. Nutzer:innen von Social-Media-Plattformen müssen im Verlauf verschiedener Stufen der Datenverarbeitungstätigkeiten jeweils ihre Einwilligung erteilen, beispielsweise bevor sie personalisierte Werbung erhalten. Wie bereits in den Leitlinien des EDSA über die gezielte Ansprache von Nutzer:innen sozialer Medien dargelegt wurde, kann die Einwilligung nur dann eine geeignete Rechtsgrundlage darstellen, wenn einer betroffenen Person Kontrolle und eine echte Wahlmöglichkeit angeboten werden⁵⁵. Darüber hinaus muss die Einwilligung gemäß Artikel 4 Nummer 11 DS-GVO für den bestimmten Fall, in informierter Weise und unmissverständlich abgegeben worden sein⁵⁶. Hierbei ist zu betonen, dass die Anforderungen an eine gültige Einwilligung gemäß der DS-GVO keine zusätzliche Verpflichtung darstellen, sondern Voraussetzungen für die rechtmäßige Verarbeitung der personenbezogenen Daten der Nutzer:innen sind. Darüber hinaus gilt für Online-Marketing oder Online-Tracking die Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation [ePrivacy-Richtlinie]). Die Voraussetzungen für eine gültige Einwilligung gemäß der

⁵⁵ Leitlinien 8/2020 für die gezielte Ansprache von Nutzer:innen sozialer Medien, Rn. 51.

⁵⁶ Siehe auch Rn. 25-29.

Datenschutzrichtlinie für elektronische Kommunikation sind jedoch identisch mit den in der DS-GVO enthaltenen Bestimmungen bezüglich der Einwilligung⁵⁷.

100. In Anbetracht des in Artikel 5 Absatz 2 DS-GVO verankerten Grundsatzes der Rechenschaftspflicht und der Notwendigkeit für den Verantwortlichen, nachzuweisen, dass die betroffenen Personen gemäß Artikel 7 Absatz 1 DS-GVO in die Verarbeitung ihrer personenbezogenen Daten eingewilligt haben, ist es von entscheidender Bedeutung, dass der Social-Media-Anbieter darlegen kann, dass er die Einwilligung der Nutzer:innen ordnungsgemäß eingeholt hat. Diese Bedingung eines Nachweises kann zu einer Herausforderung werden, wenn Nutzer:innen beispielsweise ihre Einwilligung erteilen sollen, indem sie Cookies akzeptieren. Darüber hinaus sind sich die betroffenen Personen möglicherweise nicht immer darüber im Klaren, dass sie ihre Einwilligung erteilen, wenn sie rasch eine hervorgehobene Schaltfläche oder voreingestellte Optionen anklicken. Wie jedoch in Artikel 7 Absatz 1 DS-GVO betont wird, liegt die Beweislast dafür, dass die Nutzer:innen ihre Einwilligung freiwillig erteilt haben, beim Verantwortlichen.

b. Irreführende Gestaltungsmuster

i. Inhaltsbezogene Muster

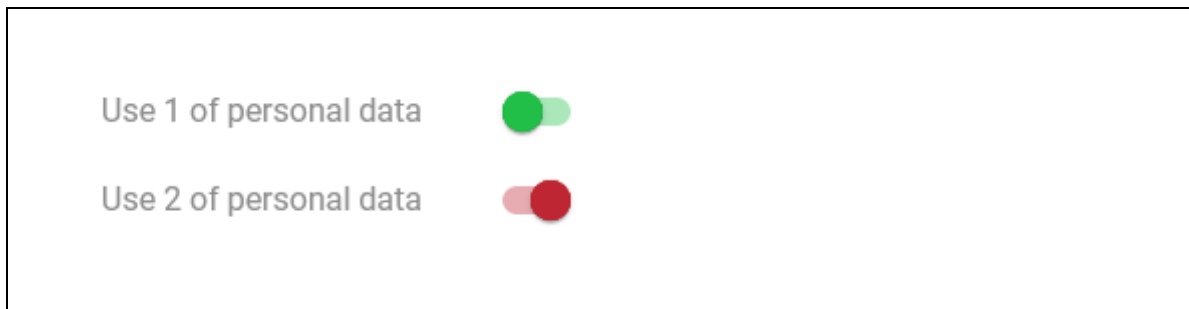
101. Zusätzlich zu den bereits erläuterten inhaltsbezogenen Mustern, die für die Informationen im Zusammenhang mit einem Ersuchen um Einwilligung gelten könnten,⁵⁸ gibt es bezüglich der Einwilligung zwei weitere inhaltsbezogene irreführende Gestaltungsmuster.

Widersprüchliche Informationen – Im Dunkeln gelassen (Anhang I Checkliste 4.6.2)

Beispiel 26: Die Benutzeroberfläche verwendet einen Schiebeschalter, der es den Nutzer:innen ermöglicht, ihre Einwilligung zu erteilen oder zu widerrufen. Die Gestaltungsweise des Schiebeschalters lässt jedoch nicht klar erkennen, in welcher Position er sich befindet und ob die Nutzer:innen ihre Einwilligung erteilt haben oder nicht. Die Stellung des Schiebeschalters stimmt nämlich nicht mit seiner Farbe überein. Befindet sich der Schalter rechts, was in der Regel mit der Aktivierung der betreffenden Funktion verbunden ist („Einschalten“), ist die Farbe des Schalters rot, was in der Regel bedeutet, dass eine Funktion ausgeschaltet ist. Umgekehrt ist dann, wenn der Schalter auf der linken Seite steht, was in der Regel bedeutet, dass die Funktion ausgeschaltet ist, die Hintergrundfarbe des Schiebeschalters grün, was normalerweise mit einer aktiven Option verbunden ist.

⁵⁷ Siehe Artikel 2 Buchstabe f der Richtlinie 2002/58/EG sowie EDSA, Stellungnahme 5/2019 zum Zusammenspiel zwischen der Datenschutzrichtlinie für elektronische Kommunikation und der DS-GVO, insbesondere in Bezug auf die Zuständigkeiten, Aufgaben und Befugnisse der Datenschutzbehörden, angenommen am 12. März 2019, Rn. 14, https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52019-interplay-between-eprivacy_de.

⁵⁸ Siehe Anwendungsfall 1, Rn. 32-49 oder die im Anhang aufgeführten Nummern der Beispiele zu Anwendungsfall 1.



102. Die Bereitstellung **widersprüchlicher Informationen** bei der Einholung der Einwilligung lässt diese unklar und unverständlich werden. Das vorstehende Beispiel veranschaulicht einen Fall, in dem die visuellen Informationen mehrdeutig sind. In der Tat werden Nutzer:innen, wenn sie mit solchen Schiebeschaltern konfrontiert sind, nicht sicher sein, ob sie ihre Einwilligung erteilt haben oder nicht. Werden visuelle Anzeiger auf solche Weise durcheinandergebracht oder in anderen Farben dargestellt, die der tatsächlichen Einstellung zu widersprechen scheinen – wie in Beispiel 26, das nur eine Illustration verwirrender Schiebeschalter enthält –, kann die Einwilligung nicht als im Sinne von Artikel 7 Absatz 2 DS-GVO in Verbindung mit Artikel 4 Nummer 11 DS-GVO unmissverständlich erteilt angesehen werden. Wie im Folgenden gezeigt wird, können **widersprüchliche Informationen** auch in Textform übermittelt werden.

Beispiel 27: Der Social-Media-Anbieter übermittelt den Nutzer:innen widersprüchliche Informationen. Obwohl in den Informationen zunächst behauptet wird, dass Kontakte nicht ohne Einwilligung importiert werden, wird gleichzeitig in einem Pop-up-Informationsfenster erläutert, wie Kontakte trotzdem importiert werden.

Behindern – Irreführende Handlung (Anhang I Checkliste 4.4.3)

103. Neben der Bereitstellung **widersprüchlicher Informationen** können die Verantwortlichen Informationen einsetzen, die dadurch verwirren, dass sie den Erwartungen der Nutzer:innen nicht entsprechen. Eine **irreführende Handlung** liegt vor, wenn eine Diskrepanz zwischen den Informationen und Handlungen, die Nutzer:innen zur Verfügung stehen, diese dazu bringt, etwas zu tun, was sie nicht beabsichtigen. Die Differenz zwischen dem, was die Nutzer:innen erwarten, und dem, was sie bekommen, wird sie voraussichtlich davon abhalten, fortzufahren.

Beispiel 28: Nutzer:innen stöbern durch ihre Feeds in sozialen Medien. Während dieses Vorgangs wird ihnen Werbung angezeigt. Fasziniert von einer Werbeanzeige klicken sie aus Neugier darüber, weshalb sie ihnen angezeigt wird, auf ein „?“-Symbol in der rechten unteren Ecke der Werbeanzeige. Es öffnet sich ein Pop-in-Fenster, in dem erläutert wird, warum die Nutzer:innen diese besondere Anzeige sehen und in dem die Kriterien für die gezielte Ansprache aufgelistet werden. Außerdem werden die Nutzer:innen in dem Pop-in-Fenster darüber informiert, dass sie ihre Einwilligung zu gezielter Werbung widerrufen können, und es wird ein Link dazu bereitgestellt. Wenn Nutzer:innen diesen Link anklicken, werden sie zu einer völlig anderen Website weitergeleitet, die allgemeine Erläuterungen dazu enthält, was eine Einwilligung ist und wie sie verwaltet wird.

104. Der vorstehende Fall veranschaulicht Inhalte, die nicht den Erwartungen der Nutzer:innen entsprechen. Wenn Nutzer:innen auf den Link klicken, würden sie erwarten, dass sie zu einer Seite weitergeleitet werden, auf der sie ihre Einwilligung direkt widerrufen können. Die Seite, die ihnen angezeigt wird, ermöglicht ihnen dies jedoch nicht und enthält auch keine konkrete Erläuterung, wie sie ihre Einwilligung auf der Social-Media-Plattform widerrufen können. Diese Diskrepanz zwischen dem, was die Nutzer:innen eigentlich vorfinden sollten, und dem, was sie tatsächlich vorfinden, ist geeignet, sie zu verwirren und sie im Ungewissen über ihr weiteres Vorgehen zu lassen. Im schlimmsten Fall könnten sie glauben, dass sie ihre Einwilligung nicht widerrufen können. Eine solche **irreführende Handlung** kann nicht als transparent im Sinne von Artikel 12 Absatz 1 DS-GVO angesehen werden. Bei einem Vergleich des Widerrufs mit der Art und Weise der Einholung der Einwilligung könnte diese Praxis einen Verstoß gegen Artikel 7 Absatz 3 DS-GVO darstellen, wenn sich der Widerruf der Einwilligung als schwieriger erweist als ihre Erteilung.
105. Wenn Social-Media-Anbieter Nutzer:innen darüber informieren, dass eine Handlung ihrerseits eine gewisse Folge haben kann, die Handlung tatsächlich aber zu einem anderen Ergebnis führt, stellt dies eine **irreführende Handlung** dar, wie das folgende Beispiel zeigt.

Beispiel 29: In dem Teil des Nutzerkontos, in dem die Nutzer:innen Gedanken, Bilder usw. teilen können, werden sie gebeten, zu bestätigen, dass sie diesen Inhalt teilen möchten, sobald sie ihn eingegeben oder hochgeladen haben. Die Nutzer:innen können zwischen einer Schaltfläche „Ja, bitte“ und einer anderen Schaltfläche „Nein, danke“ wählen. Wenn die Nutzer:innen sich jedoch gegen die Weitergabe der Inhalte an Andere entscheiden, indem sie auf die zweite Schaltfläche klicken, werden die Inhalte auf ihrem Konto veröffentlicht.

106. Wie im vorangegangenen Beispiel sind diese Informationen nicht transparent und berauben die Nutzer:innen ihrer Wahlmöglichkeiten. Auch wenn die Nutzer:innen die Veröffentlichung schnell erkennen und erneut löschen könnten, wurden die Daten trotz ihrer Ablehnung verarbeitet und Anderen zur Verfügung gestellt. Ein schlimmeres Beispiel liegt vor, wenn die Verarbeitung für die Nutzer:innen nicht oder nur mit Schwierigkeiten oder mit IT-Kenntnissen erkennbar ist, da sie im Hintergrund der Social-Media-Plattformerfolgt.

ii. Oberflächenbezogene Muster

107. Von den beiden oben aufgeführten irreführenden Gestaltungsmustern sind in diesem Anwendungsfall hauptsächlich oberflächenbasierte Muster relevant.

Überspringen – „Schau, dort drüben“ (Anhang I Checkliste 4.2.2)

108. Wenn eine datenschutzbezogene Handlung oder Information in Konkurrenz zu einem anderen Element (mit oder ohne Bezug zum Datenschutz) gebracht wird, besteht dann, wenn Nutzer:innen diese andere Option wählen, die Wahrscheinlichkeit, dass sie die erste Option vergessen, selbst wenn diese ihrer ursprünglichen Absicht entsprach. Dies ist ein Muster des Typs „**Schau, dort drüben**“, das im Rahmen einer Einzelfallprüfung bewertet werden muss.

Beispiel 30: In einem Cookie-Banner auf der Social-Media-Plattform heißt es: „Für leckere Cookies brauchen Sie nur Butter, Zucker und Mehl. Probieren Sie einmal unser Lieblingsrezept hier [Link]. Wir verwenden auch Cookies. Weitere

Informationen über unsere Cookie-Richtlinien finden Sie hier [Link]“, neben einer Schaltfläche „Okay“.

109. Humor sollte nicht dazu verwendet werden, die potenziellen Risiken falsch darzustellen und die tatsächlichen Informationen zu entwerten. In diesem Beispiel könnten die Nutzer:innen versucht sein, nur auf den ersten Link zu klicken, das Cookie-Rezept zu lesen und dann auf die Schaltfläche „Okay“ zu klicken. Abgesehen davon, dass den Nutzer:innen kein Mittel zur Verweigerung der Einwilligung zur Verfügung gestellt wird, veranschaulicht dieses Beispiel einen Fall, in dem der Einwilligung möglicherweise keine ordnungsgemäße Informiertheit zugrunde liegt. Nutzer:innen könnten meinen, dass sie mit dem Klick auf die Schaltfläche „Okay“ einfach eine lustige Meldung über Cookies als Gebäck verwerfen, und die technische Bedeutung des Begriffs „Cookies“ außer Acht lassen. In diesem Fall würde es sich nicht um eine Einwilligung in informierter Weise im Sinne von Artikel 7 Absatz 2 DS-GVO in Verbindung mit Artikel 4 Nummer 11 DS-GVO handeln.
110. In Artikel 7 Absatz 2 DS-GVO ist ferner festgelegt, dass ein Ersuchen um Einwilligung klar von anderen Sachverhalten zu unterscheiden sein muss. Daher dürfen die Datenschutzinformationen nicht durch andere Kontexte überschattet werden. In diesem Beispiel kann das auf dem Teekesselchen-Wort „Cookie“ basierende Wortspiel dazu führen, dass der Kontext Backen den Kontext Datenschutz überstrahlt. Damit die Informationen klar unterscheidbar sind, sollten die einschlägigen Informationen, die die Nutzer:innen zur Erteilung einer wirksamen Einwilligung benötigen, ganz vorne stehen, nicht **vor aller Augen verborgen** sein und nicht mit anderen Sachverhalten oder Bedeutungen vermischt werden. Es darf keine Vermengung zwischen Informationen zum Datenschutz und anderen Inhalten bestehen. Andernfalls könnten Nutzer:innen von den tatsächlichen Auswirkungen der Verarbeitung ihrer personenbezogenen Daten abgelenkt werden. Bei der Umsetzung dieser Voraussetzungen muss den Gestalter:innen ein gewisser Spielraum zur ansprechenden Gestaltung der Informationen eingeräumt werden.

Behindern – Sackgasse (Anhang I Checkliste 4.4.1)

111. Verwirrung oder Ablenkung ist hinsichtlich der Einwilligung nicht die einzige mögliche Auswirkung von irreführenden Gestaltungsmustern. Insbesondere können Muster des Typs **Sackgasse** auf verschiedene Weise die in Artikel 7 DS-GVO in Verbindung mit Artikel 4 Nummer 11 DS-GVO festgelegten Bedingungen für die Einwilligung beeinflussen.

Beispiel 31: Nutzer:innen möchten die Berechtigungen verwalten, die sie der Social-Media-Plattform auf der Grundlage ihrer Einwilligung erteilt haben. Sie müssen in den Einstellungen eine Seite für diese speziellen Handlungen finden und möchten die Weitergabe ihrer personenbezogenen Daten zu Forschungszwecken deaktivieren. Wenn Nutzer:innen auf das Kästchen klicken, um das Häkchen zu entfernen, geschieht auf Ebene der Benutzeroberfläche nichts und sie bekommen den Eindruck, dass die Einwilligung nicht widerrufen werden kann.

112. In diesem konkreten Beispiel könnte das Muster des Typs „**Sackgasse**“ gegen Artikel 7 Absatz 3 DS-GVO verstoßen, da die Nutzer:innen anscheinend nicht in der Lage sind, ihre Einwilligung in die Verarbeitung ihrer personenbezogenen Daten zu Forschungszwecken zu widerrufen, weil das Mittel dazu offenbar nicht funktioniert. Wenn die Handlungen der Nutzer:innen nicht ordnungsgemäß im System registriert werden, kann ein Verstoß gegen Artikel 7 Absatz 3 DS-GVO festgestellt werden. Wird die Wahl tatsächlich im System registriert, könnte die Tatsache, dass die Benutzeroberfläche die Angenommen

Handlungen der Nutzer:innen nicht widerspiegelt, als Verstoß gegen den Grundsatz der Verarbeitung nach Treu und Glauben nach Artikel 5 Absatz 1 Buchstabe a DS-GVO angesehen werden. Wenn eine Benutzeroberfläche scheinbar die Mittel zur ordnungsgemäßen Verwaltung der Einwilligung bietet, indem sie Nutzer:innen ermöglicht, ihre Einwilligung zu erteilen oder eine zuvor erteilte Einwilligung zu widerrufen, die Interaktion damit aber keine visuelle Wirkung auslöst, ist sie für Nutzer:innen irreführend und erzeugt bei ihnen Verwirrung und sogar Frustration. Eine solche Diskrepanz zwischen dem Zustand, in dem sich das System befindet, und den von der Benutzeroberfläche übermittelten Informationen sollte vermieden werden, da sie Nutzer:innen in der Regel an der Kontrolle ihrer personenbezogenen Daten hindern kann.

113. An vielen Verarbeitungstätigkeiten sind mehrere Parteien beteiligt, d. h. ein anderer (gemeinsam) Verantwortlicher oder ein anderer Auftragsverarbeiter, der neben dem Verantwortlichen oder dem Auftragsverarbeiter, mit dem die betroffene Person in direktem Kontakt steht, beteiligt ist.

Beispiel 32: Ein Social-Media-Anbieter arbeitet bei der Verarbeitung der personenbezogenen Daten seiner Nutzer:innen mit Dritten zusammen. In seiner Datenschutzerklärung stellt er die Liste dieser Dritten bereit, ohne einen Link zu den Datenschutzerklärungen jedes einzelnen von ihnen zu übermitteln. Stattdessen teilt er den Nutzer:innen lediglich mit, dass sie die Websites dieser Dritten besuchen sollen, um Informationen darüber zu erhalten, wie diese Unternehmen Daten verarbeiten und wie die Nutzer:innen ihre Rechte ausüben können.

114. Dieses Beispiel eines Musters des Typs **Sackgasse** zeigt, wie der Zugang zu Informationen über die jeweilige Verarbeitung für die Nutzer:innen erschwert wird. Da Nutzer:innen wahrscheinlich nicht alle einschlägigen Informationen über die Verarbeitung erhalten, könnte davon ausgegangen werden, dass eine solche Praxis gegen die Anforderungen des Artikels 12 Absatz 1 DS-GVO bezüglich leicht zugänglicher Informationen verstößt. Wird eine solche Praxis auf Informationen angewendet, die zur Einholung der Einwilligung bereitgestellt werden, kann sie gegen die Anforderungen an eine informierte Einwilligung nach Artikel 7 Absatz 2 in Verbindung mit Artikel 4 Nummer 11 DS-GVO verstoßen, da die Informationen zu schwer erreichbar wären und die betroffenen Personen sich infolgedessen nicht in vollem Umfang über die Folgen ihrer Wahl im Klaren wären.

Behindern – Länger als erforderlich (Anhang I Checkliste 4.4.2)

115. Nach Artikel 7 Absatz 3 DS-GVO sollte der Widerruf der Einwilligung genauso einfach sein wie die Erteilung der Einwilligung. In den Leitlinien 5/2020 zur Einwilligung gemäß Verordnung 2016/679 wird das Thema dahingehend weiter ausgeführt, dass das Erteilen und Widerrufen der Einwilligung auf demselben Weg möglich sein sollte. Dies hat zur Folge, dass dieselbe Benutzeroberfläche genutzt werden muss, bedeutet aber auch, dass die Mechanismen für den Widerruf der Einwilligung leicht zugänglich sein sollten, beispielsweise über einen Link oder ein Symbol, das während der Nutzung der Social-Media-Plattform jederzeit verfügbar ist.

Beispiel 33: Ein Social-Media-Anbieter bietet keine direkte Abwahlmöglichkeit (Opt-out) einer Verarbeitung für gezielte Werbung an, obwohl die Einwilligung (Opt-in) nur einen Klick erfordert.

116. Die Zeit oder Anzahl der Klicks, die für den Widerruf der Einwilligung erforderlich sind, kann dazu genutzt werden, zu beurteilen, ob der Widerruf tatsächlich einfach zu erreichen ist. Die Umsetzung des

in Beispiel 33 gezeigten irreführenden Gestaltungsmusters **Länger als erforderlich** im Rahmen des Nutzererlebnisses zum Widerruf der Einwilligung verstößt gegen diese Grundsätze und somit gegen Artikel 7 Absatz 3 DS-GVO.

Überfrachtung – Datenschutz-Labyrinth (Anhang Checkliste 4.1.2)

117. Wie in den Leitlinien 5/2020 zur Einwilligung hervorgehoben wird, müssen den betroffenen Personen Informationen über die Verarbeitung auf der Grundlage der Einwilligung zur Verfügung gestellt werden, damit sie eine Entscheidung in informierter Weise treffen können.⁵⁹ Ohne sie kann die Einwilligung nicht als gültig angesehen werden. In denselben Leitlinien werden die Möglichkeiten zur Bereitstellung von Informationen näher ausgeführt und es wird präzisiert, dass hierfür mehrschichtige Informationen genutzt werden können. Wie in Anwendungsfall 2a gezeigt wird⁶⁰, müssen Social-Media-Anbieter darauf achten, das irreführende Gestaltungsmuster **Datenschutz-Labyrinth** zu vermeiden, wenn sie im Zusammenhang mit einem Einwilligungsversuchen Informationen auf mehreren Ebenen bereitstellen. Wenn einige Informationen zu schwer zu finden sind, weil die betroffenen Personen durch mehrere Seiten oder Dokumente navigieren müssen, könnte die durch die Bereitstellung dieser Informationen eingeholte Einwilligung als nicht in informierter Weise erteilt angesehen werden und somit gegen Artikel 7 DS-GVO in Verbindung mit Artikel 4 Nummer 11 DS-GVO verstoßen. Im weiteren Sinne würde dies bedeuten, dass die Einwilligung ungültig ist und der Social-Media-Anbieter gegen Artikel 6 DS-GVO verstößt.

Beispiel 34: Informationen zum Widerruf der Einwilligung können über einen Link abgerufen werden, der nur zugänglich ist, wenn sämtliche Abschnitte des Kontos sowie Informationen im Zusammenhang mit Werbung, die im Feed des sozialen Mediums angezeigt werden, geprüft werden.

118. Wie das vorstehend beschriebene Szenario zeigt, kann das irreführende Gestaltungsmuster **Datenschutz-Labyrinth** auch nach der Einholung der Einwilligung ein Problem darstellen, wenn die Bedingung nach Artikel 7 Absatz 3 Satz 4 DS-GVO, wonach der Widerruf der Einwilligung so einfach sein muss wie die Erteilung der Einwilligung, nicht erfüllt wird. Dies ist insbesondere darauf zurückzuführen, dass das Verfahren des Einwilligungswiderrufs mehr Schritte umfasst als die bestätigende Handlung der Einwilligung. Da zudem die bereitgestellten Informationen für die betroffene Person nicht leicht zugänglich sind, da sie über verschiedene Teile der Seite verteilt sind, wird gegen den Grundsatz des Artikels 12 Absatz 1 DS-GVO verstoßen.

Überfrachtung – Ständige Aufforderungen (Anhang I Checkliste 4.1.1)

119. **Ständige Aufforderungen** stellen eine Behinderung bei der regulären Nutzung sozialer Medien dar, wenn sie bei Nutzer:innen eingesetzt werden, die der Verarbeitung ihrer personenbezogenen Daten für einen bestimmten Zweck nicht zugestimmt haben. Dies bedeutet, dass die Nutzer:innen ihre Einwilligung nicht verweigern und im weiteren Sinne nicht widerrufen können, ohne dass ihnen dadurch Nachteile entstehen. Dies steht im Widerspruch zur Bedingung der freiwillig erteilten Einwilligung nach Artikel 7 in Verbindung mit Artikel 4 Nummer 11 DS-GVO, wonach unter Einwilligung jede freiwillig abgegebene Willensbekundung der betroffenen Person zu verstehen ist, mit der sie zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten

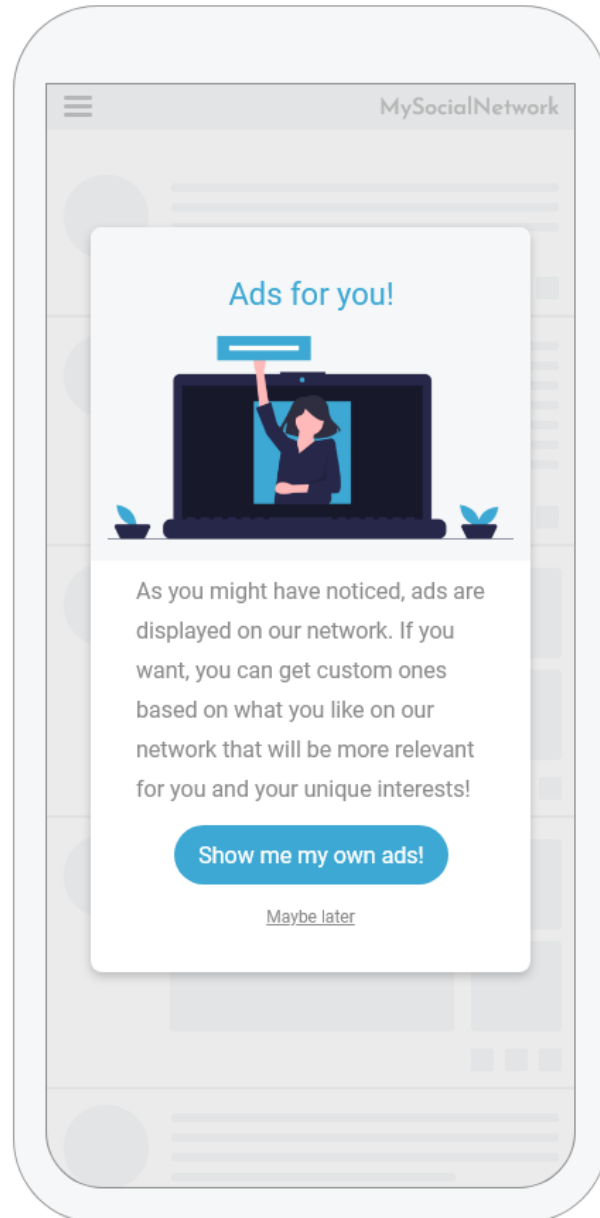
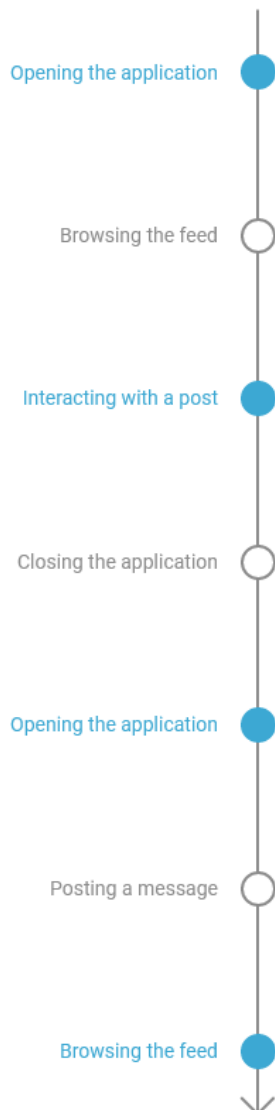
⁵⁹ Leitlinien 5/2020 zur Einwilligung, Rn. 62-64.

⁶⁰ Siehe Rn. 79-81.

einverstanden ist. Gemäß Erwägungsgrund 42 Satz 5 DS-GVO gilt eine Einwilligung ferner nicht als freiwillig erteilt, wenn die Nutzer:innen keine echte oder freie Wahl haben. Dies wird auch durch die EDSA-Leitlinien zur Einwilligung unterstützt, in denen dargelegt wird, dass die Einwilligung nicht gültig ist, wenn die betroffenen Personen keine wirkliche Wahl haben oder sich aufgrund unangemessenen Drucks oder unangemessener Einflussnahme zur Einwilligung gedrängt fühlen, wodurch sie an der Ausübung ihres freien Willens gehindert werden.⁶¹ Da **ständige Aufforderungen** einen solche Art von Druck erzeugen können, verstößt dies gegen den Grundsatz der freiwillig erteilten Einwilligung. Da es darüber hinaus unwahrscheinlich ist, dass der Social-Media-Anbieter, sobald die Nutzer:innen ihre Einwilligung erteilt haben, regelmäßig (z. B. jedes Mal, wenn sie sich erneut in ihr Konto einloggen) die Möglichkeit zum Widerruf der Einwilligung bieten wird, kann dieses irreführende Gestaltungsmuster gegen Artikel 7 Absatz 3 Satz 4 DS-GVO verstoßen, wonach der Widerruf der Einwilligung genauso einfach sein muss wie ihre Erteilung („Spiegeleffekt“).

⁶¹ Leitlinien 5/2020 zur Einwilligung, Rn. 13-14.

Timeline of the user interactions
where the **pop-up is displayed**



Beispiel 35: In diesem Beispiel werden Nutzer:innen bei der Erstellung ihres Kontos gefragt, ob sie akzeptieren, dass ihre Daten verarbeitet werden, damit sie personalisierte Werbung erhalten. Falls Nutzer:innen bei der Anmeldung nicht in diese Nutzung ihrer Daten einwilligen, sehen sie regelmäßig – während der Nutzung des sozialen Netzwerks – das vorstehend dargestellte Kästchen, in dem sie gefragt werden, ob sie personalisierte Werbung wünschen. Dieses Kästchen blockiert sie bei der Nutzung des sozialen Netzwerks. Da sie regelmäßig angezeigt wird, ist davon auszugehen, dass diese **ständige Aufforderung** die Nutzer:innen ermüdet und dazu bringt, in personalisierte Werbung einzuwilligen. Darüber hinaus wird in dieser Schnittstelle auch das Gestaltungsmuster **Vor aller Augen**

verborgen⁶² verwendet, da die Handlung, mit der Werbung akzeptiert wird, viel stärker sichtbar ist als die Option zu deren Ablehnung.

120. Darüber hinaus könnte der Verantwortliche gegen den Grundsatz der Verarbeitung nach Treu und Glauben im Sinne von Artikel 5 Absatz 1 Buchstabe a DS-GVO verstoßen. In Anbetracht dessen, dass im vorstehenden Beispiel die Nutzer:innen bei der Erstellung ihres Kontos nicht durch eine unmissverständliche Handlung in die Verarbeitung ihrer personenbezogenen Daten für gezielte Werbung eingewilligt haben, ist die wiederholte Eingabeaufforderung, mit der eine von ihnen vorgenommene eindeutige Ablehnung ständig infrage gestellt wird, belastend. Diese eindeutige Handlung, die die Nutzer:innen während des Registrierungsverfahrens vornahmen, wird nun ständig infrage gestellt. Die dadurch herbeigeführte Verschlechterung der Nutzererfahrung erhöht in erheblichem Maße die Wahrscheinlichkeit, dass Nutzer:innen die gezielte Werbung irgendwann akzeptieren, um zu vermeiden, dass sie jedes Mal erneut gefragt werden, wenn sie sich in ihr Konto einloggen und die Social-Media-Plattform nutzen möchten. In diesem Fall wirkt sich die Verweigerung der Einwilligung unmittelbar auf die Qualität der den Nutzer:innen erbrachten Dienstleistung und die Beschaffenheit der Vertragserfüllung aus.

c. Best Practices

Geräteübergreifende Einheitlichkeit: Ist die Social-Media-Plattform mittels verschiedener Geräte (z. B. Computer, Smartphone usw.) verfügbar, sollten sich die Einstellungen und Informationen bezüglich des Datenschutzes in den verschiedenen Versionen an denselben Orten befinden und über dieselben Pfade und Elemente in der Benutzeroberfläche (Menüs, Symbole usw.) zugänglich sein.

Änderungshistorien und Vergleich: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 29).

Einheitliche Formulierungen: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 29).

Begriffsbestimmungen bereitstellen: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 29).

Verwendung von Beispielen: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 30).

Angeheftete Navigationsleiste: Eine Begriffsbestimmung ist im Anwendungsfall 2a zu finden (S. 36).

Zurück zum Seitenanfang: Eine Begriffsbestimmung ist im Anwendungsfall 2a zu finden (S. 37).

Benachrichtigungen: Eine Begriffsbestimmung ist im Anwendungsfall 2c zu finden (S. 42).

Folgen erläutern: Eine Begriffsbestimmung ist im Anwendungsfall 2c zu finden (S. 42).

Anwendungsfall 3b: Verwalten der Datenschutzeinstellungen

a. Beschreibung des Kontextes

121. Nutzer:innen sollten nach Abschluss des Anmeldeverfahrens und während des gesamten Lebenszyklus ihres Kontos in sozialen Medien in der Lage sein, ihre Datenschutzeinstellungen anzupassen.
122. Unabhängig davon, ob die Nutzer:innen bereits Kenntnisse über den Datenschutz im Allgemeinen und die DS-GVO im Besonderen haben und ob sie auf die personenbezogenen Daten achten, die sie

⁶² Siehe Randnummern. 49 oder Teil 4.3.2 des Anhangs.

weitergeben wollen oder nicht und von denen sie möchten, dass andere sie sehen, haben sie alle das Recht, bei der Nutzung sozialer Medien transparent über ihre Möglichkeiten informiert zu werden.

123. Nutzer:innen teilen auf Social-Media-Plattformen eine große Zahl personenbezogener Daten. Häufig werden sie von den Plattformen ermutigt, noch mehr Informationen zu teilen. Nutzer:innen möchten vielleicht nur Momente ihres Lebens teilen, an einer Debatte über ein Thema teilnehmen oder ihre Kontaktnetze aus beruflichen oder persönlichen Gründen erweitern. Ihnen müssen jedoch auch die Instrumente an die Hand gegeben werden, mit denen sie kontrollieren können, wer welche Teile ihrer personenbezogenen Daten sehen kann. Eine Möglichkeit, mit der ein Vervielfachen der Zahl der für eine Änderung von Einstellungen erforderlichen Schritte vermieden werden kann, könnte darin bestehen, ein Datenschutz-Dashboard zu entwickeln, das die Einstellungen zentral ermöglicht und die Kontrolle der Nutzerdaten erleichtert.

b. Maßgebliche Rechtsvorschriften

124. Wie bereits erwähnt⁶³ wird in Artikel 5 Absatz 1 Buchstabe a DS-GVO als einer der wichtigsten Grundsätze für die Verarbeitung personenbezogener Daten festgelegt, dass personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und – in dieser Hinsicht besonders wichtig – in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“). Nach dem Grundsatz der Rechenschaftspflicht gemäß Artikel 5 Absatz 2 DS-GVO müssen Verantwortliche darlegen, welche Maßnahmen sie ergreifen, um ihre Verarbeitungstätigkeiten nicht nur rechtmäßig und nach Treu und Glauben, sondern auch transparent zu gestalten. Darüber hinaus sind in diesem Anwendungsfall die Grundsätze der Datenminimierung nach Artikel 5 Absatz 1 Buchstabe c und des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen nach Artikel 25 DS-GVO relevant.

c. Irreführende Gestaltungsmuster

i. Inhaltsbezogene Muster

125. Das erste Problem, dem Nutzer:innen in diesem Zusammenhang begegnen, ist die Frage, wo sie Einstellungen, die den Datenschutz betreffen, tatsächlich finden können. Nutzer:innen lesen vielleicht die Datenschutzhinweise und beschließen dann, Änderungen im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten vorzunehmen. Sie könnten dies auch tun, ohne die Datenschutzhinweise gelesen zu haben, einfach mittels ihrer regelmäßigen Nutzung der sozialen Medien, beispielsweise wenn sie erkennen, dass eine auf der Social-Media-Plattform veröffentlichte Information (z. B. ein Foto der Familie am Strand) an eine unerwünschte Personengruppe (z. B. Arbeitskollegen) weitergegeben wird. Der Grundsatz der Transparenz verlangt in jedem Fall, dass die Einstellungsoptionen leicht zugänglich und in verständlicher Weise verfügbar sein müssen. Dies ließe sich dadurch erreichen, dass die Daten und Datenschutzeinstellungen mithilfe einer selbsterklärenden URL wie [soziales-netzwerk.com]/datenschutzeinstellungen zentral an einem Ort zusammengefasst werden.
126. Im Zusammenhang mit diesem Thema gibt es mehrere Gestaltungsmuster, die den Nutzer:innen das Auffinden der Einstellungen erschweren. Die Gestalter:innen von Social-Media-Plattformen sollten daher darauf achten, diese irreführenden Gestaltungsmuster zu vermeiden.

⁶³ Siehe Rn. 1, 9, 10, 14-16.

Überfrachtung – Zu viele Optionen (Anhang I Checkliste 4.1.3)

127. Datenschutzeinstellungen müssen leicht zugänglich und logisch angeordnet sein. Einstellungen, die sich auf denselben Datenschutzaspekt beziehen, sollten sich vorzugsweise an einer einzigen, markanten Stelle befinden. Andernfalls sehen sich die Nutzer:innen einer zu großen Zahl von Seiten gegenüber, die sie prüfen und durchsehen müssen, was sie bei der Einstellung ihrer Datenschutzpräferenzen überfordert. Werden sie mit **zu vielen Optionen** konfrontiert, aus denen sie auswählen können, kann das dazu führen, dass sie nicht mehr in der Lage sind, überhaupt eine Wahl zu treffen, oder dass sie einige Einstellungen übersehen, sodass sie schließlich aufgeben oder die Einstellung ihrer Datenschutzpräferenzen versäumen. Dies verstößt gegen die Grundsätze der Transparenz und der Verarbeitung nach Treu und Glauben. Insbesondere kann dies einen Verstoß gegen Artikel 12 Absatz 1 DS-GVO darstellen, da entweder eine spezifische Überprüfung im Zusammenhang mit dem Datenschutz durch die Verteilung auf mehrere Seiten erschwert wird oder der Unterschied zwischen den verschiedenen Optionen, die den Nutzer:innen zur Verfügung gestellt werden, nicht deutlich gemacht wird.

Beispiel 36: Die Nutzer:innen wissen wahrscheinlich nicht, was zu tun ist, wenn das Menü einer Social-Media-Plattform mehrere Tabs enthält, die sich mit Datenschutz befassen, beispielsweise: „Datenschutz“, „Sicherheit“, „Inhalt“, „Schutz der Privatsphäre“, „Ihre Präferenzen“.

128. In diesem Beispiel geben die Titel der Tabs nicht eindeutig an, welche Inhalte die Nutzer:innen auf der zugehörigen Seite erwarten können, oder dass sich alle Tabs auf den Datenschutz beziehen, insbesondere dann, wenn eine der Tabs ausdrücklich diese Bezeichnung trägt. Dadurch kann das Risiko entstehen, dass Nutzer:innen daran gehindert werden, Änderungen vorzunehmen. Wenn sie beispielsweise die Zahl der Personen, die die von ihnen hochgeladenen Bilder sehen können, einschränken oder erweitern möchten, könnten die Bezeichnungen der Tabs sie dazu veranlassen, entweder auf „Sicherheit“ zu klicken, wenn sie der Ansicht sind, dass mit der Veröffentlichung ihrer Daten Sicherheitsrisiken verbunden sind, auf „Inhalt“, da die Nutzer:innen die Sichtbarkeit ihres Posts festlegen möchten, oder auf „Schutz der Privatsphäre“, da sich dieser spezielle Begriff unmittelbar auf das bezieht, was Menschen mit anderen teilen möchten. Dies bedeutet, dass diese Titel im Hinblick auf die Handlung, die die Nutzer:innen ausführen möchten, nicht klar genug sind. Insbesondere werden die Begriffe „Datenschutz“ und „Schutz der Privatsphäre“ häufig als Synonyme verwendet, was sie besonders verwirrend macht, wenn sie als unterschiedliche Abschnitte dargestellt werden.

Im Dunkeln gelassen – Widersprüchliche Informationen (Anhang I Checkliste 4.6.2)

129. Wie bereits in Beispiel 12 beschrieben wurde und im folgenden Beispiel ausführlicher dargestellt wird, können Nutzer:innen auch im Rahmen der Datenschutzeinstellungen **Widersprüchliche Informationen** erhalten.

Beispiel 37: Nutzer:in X schaltet die Nutzung seines geografischen Standorts für Werbezwecke aus. Nachdem er den Schiebeschalter, der dies ermöglicht, angeklickt hat, erscheint eine Nachricht mit dem Hinweis „Wir haben Ihren geografischen Standort deaktiviert, aber Ihr Standort wird weiterhin genutzt.“

Überfrachtung – Datenschutz-Labyrinth (Anhang I Checkliste 4.1.2)

130. Wenn Nutzer:innen eine Datenschutzeinstellung ändern, verpflichtet der Grundsatz der Verarbeitung nach Treu und Glauben die Social-Media-Anbieter auch dazu, die Nutzer:innen über andere, ähnliche Einstellungen zu informieren. Sind solche Einstellungen über verschiedene, nicht miteinander verbundene Seiten der Social-Media-Plattform verteilt, werden die Nutzer:innen wahrscheinlich ein oder mehrere Mittel zur Kontrolle eines Aspekts ihrer personenbezogenen Daten übersehen. Nutzer:innen erwarten, dass sie verwandte Einstellungen nebeneinander finden.

Beispiel 38: Verwandte Themen wie die Einstellungen für die Weitergabe von Daten durch den Anbieter an Dritte und umgekehrt werden nicht an denselben oder nahe beieinander liegenden Orten bereitgestellt, sondern in verschiedenen Tabs des Einstellungsmenüs.

131. Hinsichtlich der durchschnittlichen Anzahl von Schritten, die für die Nutzer:innen von Social-Media-Plattformen bei der Änderung einer Einstellung noch tragbar sind, gibt es keinen für alle passenden allgemeingültigen Ansatz. Gleichzeitig kann eine größere Zahl von Schritten die Nutzer:innen davon abhalten, die Änderung abzuschließen, oder dazu führen, dass sie einen Teil der Änderung übersehen, insbesondere wenn sie mehrere Änderungen vornehmen wollen. Den Willen der Nutzer:innen auf solche Weise zu behindern, verstößt gegen die Grundsätze von Treu und Glauben nach Artikel 5 Absatz 1 Buchstabe a DS-GVO. Darüber hinaus ist eine Änderung der Einstellungen eng mit der Ausübung der Rechte betroffener Personen verbunden.⁶⁴ Die Änderung einer datenbezogenen Einstellung, z. B. die Berichtigung des eigenen Namens oder die Löschung des Abschlussjahres, kann als Ausübung des Rechts auf Berichtigung bzw. des Rechts auf Löschung dieser speziellen Daten betrachtet werden. Die Zahl der erforderlichen Schritte sollte daher so gering wie möglich sein. Auch wenn sie variieren kann, behindert eine übermäßige Anzahl von Schritten die Nutzer:innen und verstößt daher gegen den Grundsatz von Treu und Glauben sowie gegen Artikel 12 Absätze 1 und 2 DS-GVO.

Unbeständig – Sprachliche Diskontinuität (Anhang I Checkliste 4.5.4)

132. Im Hinblick auf transparente Informationen müssen die Gestalter:innen von Social-Media-Plattformen auch darauf achten, die in Anwendungsfall 2a aufgeführten inhaltsbezogenen irreführenden Gestaltungsmuster wie z. B. **Sprachliche Diskontinuität** zu vermeiden. Werden die Einstellungsseiten (oder Teile davon) nicht in der Sprache zur Verfügung gestellt, die Nutzer:innen für die Plattform gewählt haben, wird es ihnen erschwert, zu verstehen, was sie ändern können und wie sie folglich ihre Präferenzen festlegen können.

Unbeständig – Uneinheitliche Benutzeroberfläche (Anhang I Checkliste 4.5.3)

133. In diesem Zusammenhang tritt ein weiteres Problem auf, wenn Social-Media-Plattformen den Nutzer:innen datenschutzfreundliche Wahlmöglichkeiten anbieten, sie aber nicht auf eine klare Art und Weise darüber informieren. Dies kann der Fall sein, wenn die Social-Media-Plattform plötzlich von ihrem üblichen Gestaltungsmuster abweicht. Eine solche **uneinheitliche Schnittstelle** liegt vor, wenn eine Benutzeroberfläche in verschiedenen Kontexten uneinheitlich ist oder mit den Erwartungen der Nutzer:innen nicht übereinstimmt. Diese Unterschiede können dazu führen, dass Nutzer:innen die gewünschte Kontrollfunktion oder Information nicht finden oder dass sie aus reiner Gewohnheit mit

⁶⁴ Siehe die Anwendungsfälle 4 und 5, d. h. Teile 3.4 und 3.5 dieser Leitlinien.

einem Element der Benutzeroberfläche interagieren, obwohl diese Interaktion zu einer Datenschutzentscheidung führt, die die Nutzer:innen nicht wünschen.

Beispiel 39: Auf der gesamten Social-Media-Plattform werden neun von zehn Datenschutzeinstellungen in der folgenden Reihenfolge dargestellt:

- restriktivste Option (d. h. Austausch der geringsten Menge an Daten mit Anderen)
- beschränkte Option, jedoch nicht so restriktiv wie die erste Option

– am wenigsten restriktive Option (d. h. Austausch der größten Menge an Daten mit Anderen).

Die Nutzer:innen dieser Plattform sind es gewohnt, dass ihre Datenschutzeinstellungen in dieser Reihenfolge dargestellt werden. Diese Reihenfolge wird jedoch bei der letzten Einstellung nicht angewendet. Dort wird die Wahl der Sichtbarkeit der Geburtstage der Nutzer:innen stattdessen in folgender Reihenfolge dargestellt:

- Meinen Geburtstag vollständig anzeigen: 15. Januar 1929 (= am wenigsten restriktive Option)
- Nur Tag und Monat anzeigen: 15. Januar (= beschränkte, aber nicht restriktivste Option)
- Meinen Geburtstag für niemand anderen sichtbar machen (= restriktivste Option).

134. Im Beispiel werden die drei Auswahlmöglichkeiten in der letzten Einstellung in einer anderen Reihenfolge dargestellt als in den vorherigen. Nutzer:innen, die zuvor ihre anderen Einstellungen geändert haben, sind wahrscheinlich an die „übliche“ Reihenfolge der Einstellungen eins bis neun gewöhnt. Bei der letzten Einstellung sind sie bereits so sehr an diese Reihenfolge gewöhnt, dass sie in der Annahme, dass dies die restriktivste Option sein muss, instinktiv die erste Option wählen. Die Anordnung der Optionen einer Datenschutzeinstellung in einer Weise, die sich so stark von den anderen Einstellungen auf derselben Social-Media-Plattform unterscheidet, stellt eine **uneinheitliche Benutzeroberfläche** dar, da sie mit dem spielt, was die Nutzer:innen gewohnt sind und was sie erwarten. Dies kann zu Verwirrung führen oder Nutzer:innen in dem Glauben lassen, dass sie die gewünschte Wahl getroffen haben, obwohl dies in Wirklichkeit nicht der Fall ist.

ii. Oberflächenbezogene Muster

135. Das zweite Problem, dem man im Zusammenhang mit Datenschutzeinstellungen begegnet, besteht darin, dass die Einstellungen gegen den Grundsatz des Datenschutzes durch datenschutzfreundliche Voreinstellungen verstoßen könnten. Nach Artikel 25 Absatz 1 DS-GVO müssen die Verantwortlichen geeignete Maßnahmen zur Umsetzung der Datenschutzgrundsätze wie etwa Datenminimierung treffen (Artikel 5 Absatz 1 Buchstabe c DS-GVO). Diese Bestimmungen werden nicht eingehalten, wenn bei den Einstellungen für die Weitergabe personenbezogener Daten eine der stärker invasiven Optionen statt die am wenigsten invasive Option vorgewählt wird.

Überspringen – Trügerische Bequemlichkeit (Anhang I Checkliste 4.2.1)

Beispiel 40: Zwischen den Optionen für die Sichtbarkeit der Daten „für mich sichtbar“, „für meine engsten Freunde“, „für meinen gesamten Bekanntenkreis“ und „öffentlich“ ist die mittlere Option „für meinen gesamten Bekanntenkreis“

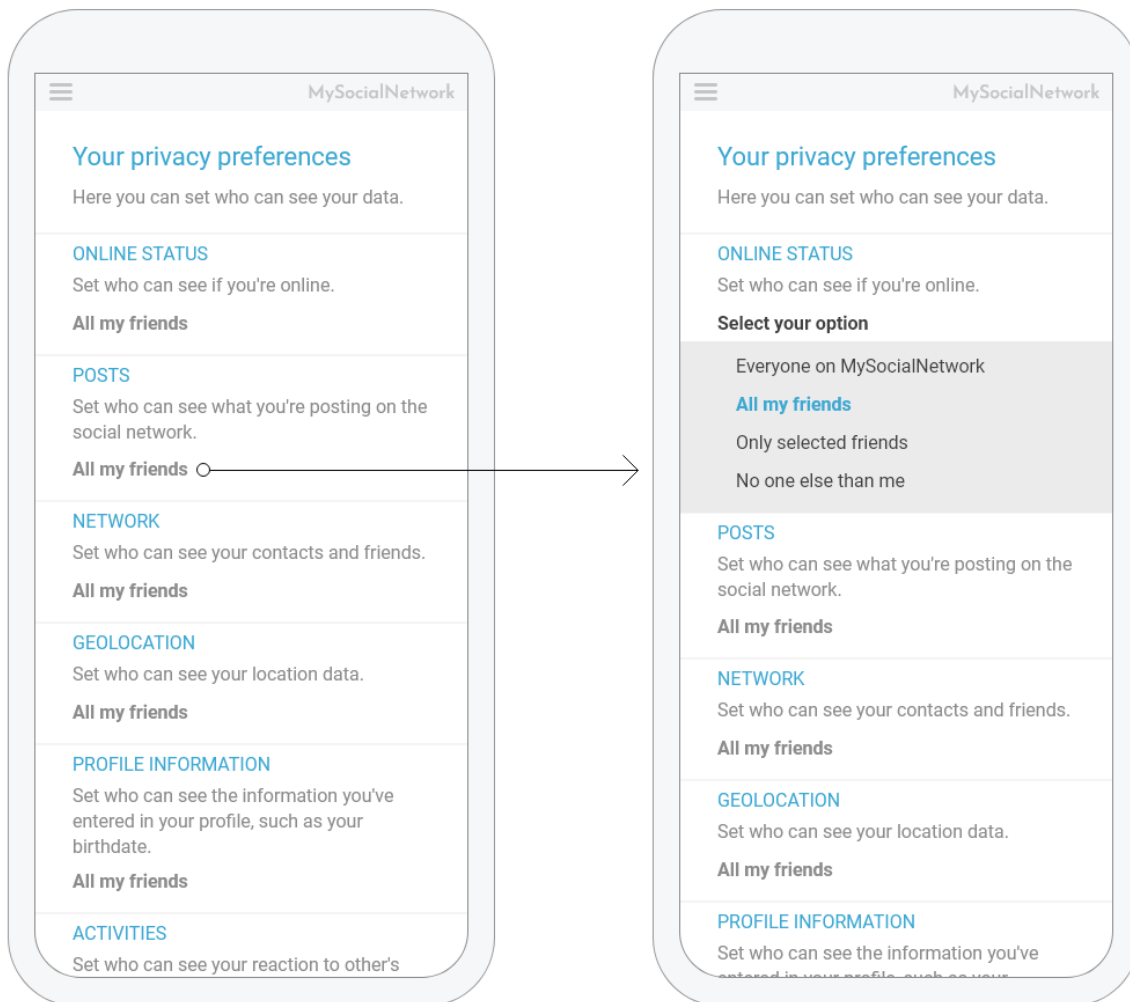
voreingestellt. Dies bedeutet, dass alle mit der betroffenen Person verbundenen Nutzer:innen deren Beiträge sowie alle zur Anmeldung auf der Social-Media-Plattform eingegebenen Informationen wie die E-Mail-Adresse oder das Geburtsdatum einsehen können.

136. Social-Media-Anbieter könnten argumentieren, dass die am wenigsten invasive Einstellung das von Nutzer:innen einer bestimmten Social-Media-Plattform verfolgte Ziel, beispielsweise von Unbekannten gefunden zu werden, um einen neuen Kumpel, ein Date oder eine Arbeitsstelle zu finden, vereiteln könnten. Auch wenn dies für bestimmte Einstellungen der Fall sein mag, müssen die Anbieter berücksichtigen, dass die Tatsache, dass Nutzer:innen bestimmte Daten in das Netz hochladen, keine Einwilligung zur Weitergabe dieser Daten an andere darstellt.⁶⁵ Wenn Anbieter den Datenschutz durch datenschutzfreundliche Voreinstellungen zurückstellen, müssen sie darauf achten, die Nutzer:innen darüber angemessen zu informieren. Dies bedeutet, dass die Nutzer:innen wissen müssen, was die Standardeinstellung ist, dass weniger invasive Optionen zur Verfügung stehen und wo auf der Plattform sie Änderungen vornehmen müssen. In dem genannten Beispiel bedeutet dies, dass dann, wenn für Beiträge, die Nutzer:innen aktiv auf der Plattform veröffentlichen, die Option „für meine engsten Freunde“ voreingestellt ist, den Nutzer:innen gezeigt werden muss, wo sie diese Einstellung ändern können. Die Voreinstellung der Sichtbarkeit auf „für den gesamten Bekanntenkreis“ (oder sogar die allgemeine Öffentlichkeit) stellt jedoch **trügerische Bequemlichkeit** dar, insbesondere wenn sie auf Daten angewendet wird, die der Social-Media-Anbieter von den Nutzer:innen für die Einrichtung eines Kontos gefordert hat, etwa die E-Mail-Adresse oder ihr Geburtsdatum. Wie in Anwendungsfall 1 in Rn. 55 beschrieben, verstößt diese Praxis gegen Artikel 25 Absatz 2 DS-GVO.

⁶⁵ Beispielsweise ihr Geburtsdatum, siehe Rn. 58.

Aufwühlen – Vor aller Augen verborgen (Anhang I Checkliste 4.3.2)

137. Die irreführenden Gestaltungsmuster **Vor aller Augen verborgen** und **Trügerische Bequemlichkeit** lassen sich im Zusammenhang mit der Auswahl datenschutzbezogener Optionen leicht kombinieren, wie dies in Beispiel 9 für das Anmeldeverfahren und in dem folgenden Beispiel, in dem Nutzer:innen während der Nutzung der sozialen Medien ihre Datenschutzpräferenzen ändern möchten, veranschaulicht wird.



Beispiel 41: In diesem Beispiel müssen Nutzer:innen, die die Sichtbarkeit ihrer Daten verwalten wollen, die Registerkarte „Datenschutzpräferenzen“ öffnen. Dort werden die Informationen, für die sie ihre Präferenz festlegen können, aufgeführt. Allerdings lässt die Art und Weise, in der die Informationen angezeigt werden, nicht deutlich erkennen, wie die Einstellungen geändert werden. Tatsächlich müssen die Nutzer:innen auf die angezeigte Sichtbarkeitsoption klicken, um auf ein Dropdown-Menü zu gelangen, in dem sie die von ihnen bevorzugte Option auswählen können.

138. Auch wenn die Möglichkeit zur Änderung der Präferenzen in diesem Tab zur Verfügung steht, ist sie **vor aller Augen verborgen**, da das Dropdown-Menü für die Nutzer:innen nicht unmittelbar zu erkennen ist. Sie müssen erraten, dass sich mit einem Klick auf die angezeigte Option etwas öffnet. Es gibt in der Tat keinen der üblichen visuellen Hinweise (unterstrichener Text, Pfeil nach unten) auf die Angenommen

Möglichkeit, zu interagieren und das Dropdown-Menü zu öffnen. Diese besondere Praxis ist den Nutzer:innen gegenüber unfair und könnte zu einem allgemeinen Verstoß gegen den Grundsatz von Treu und Glauben gemäß Artikel 5 Absatz 1 Buchstabe a DS-GVO führen. Darüber hinaus könnte bei einer standardmäßigen Vorauswahl der Optionen auch das irreführende Gestaltungsmuster **Trügerische Bequemlichkeit** festgestellt werden, wie es in Rn. 128 beschrieben wird.

Unbeständig – Dekontextualisierung (Anhang I Checkliste 4.5.2)

139. **Dekontextualisierung** findet statt, wenn sich eine Information oder Kontrollfunktion mit Bezug zum Datenschutz auf einer Seite außerhalb des Kontextes befindet, sodass es unwahrscheinlich ist, dass Nutzer:innen sie finden, da sie nicht intuitiv auf dieser speziellen Seite nach ihr suchen würden.

Beispiel 42: Die Datenschutzeinstellungen sind im Nutzerkonto schwer zu finden, da es auf der ersten Ebene kein Kapitel im Menü mit einem Namen oder einer Überschrift gibt, das in diese Richtung weist. Die Nutzer:innen müssen in anderen Untermenüs wie „Sicherheit“ nachschauen.

140. In diesem Beispiel werden die Nutzer:innen nicht zu den Datenschutzeinstellungen geführt, da keine aussagekräftigen, eindeutigen Begriffe verwendet werden, um anzugeben, wo auf der Social-Media-Plattform sich diese Einstellungen befinden. Tatsächlich umfasst der Begriff „Sicherheit“ nur einen Bruchteil dessen, was von Datenschutzeinstellungen erwartet werden kann. Daher entspricht es nicht der Intuition der Nutzer:innen, in diesem Menü nachzuschauen, um solche Einstellungen zu finden. Dieser Mangel an Transparenz gestaltet den Zugang zu Informationen schwieriger, als er sein sollte, und kann als Verstoß gegen Artikel 12 Absatz 1 DS-GVO und möglicherweise Artikel 12 Absatz 2 DS-GVO angesehen werden, wenn sich die betreffenden Einstellungen auf die Ausübung eines Rechts beziehen.

Beispiel 43: Eine Änderung von Einstellungen wird verhindert, da in der Desktop-Version der Social-Media-Plattform die Schaltfläche „Speichern“ zur Umsetzung der Änderungen nicht zusammen mit allen Optionen angezeigt wird, sondern nur am oberen Rand des Untermenüs sichtbar ist. Die Nutzer:innen werden sie wahrscheinlich übersehen und fälschlicherweise davon ausgehen, dass ihre Einstellungen automatisch gespeichert werden, sodass sie zu einer anderen Seite wechseln, ohne auf die Schaltfläche „Speichern“ zu klicken. Dieses Problem tritt in der App-Version und der Version für Mobilgeräte nicht auf. Daher schafft dies bei Nutzer:innen, die von der Version für Mobilgeräte/App zur Desktop-Version wechseln, zusätzliche Verwirrung und sie könnten zu der Annahme kommen, dass sie ihre Einstellungen nur in der Version für Mobilgeräte oder der App ändern können.

141. Wenn die Nutzer:innen die Datenschutzeinstellungen einmal gefunden und ihre Präferenzen festgelegt haben, dürfen sie daran nicht gehindert werden. Sobald Nutzer:innen eine Änderung vorgenommen haben, muss klar sein, wie sie gespeichert werden kann, unabhängig davon, ob dies sofort bei der Anpassung einer Einstellung durch die Nutzer:innen geschieht oder ob eine Bestätigung mittels Anklicken eines bestimmten Elements der Benutzeroberfläche, beispielsweise einer Schaltfläche „Speichern“, erforderlich ist. Darüber hinaus schreibt der Grundsatz von Treu und Glauben nach Artikel 5 Absatz 1 Buchstabe a DS-GVO vor, dass Social-Media-Anbieter auf ihrer gesamten Plattform, insbesondere über verschiedene Geräte hinweg, einheitlich sein müssen. Dies ist nicht der Fall, wenn die Benutzeroberfläche eines der in den vorstehenden Beispielen beschriebenen irreführenden Gestaltungsmuster verwendet.

d. Best Practices

Datenschutzverzeichnis: Um eine einfache Orientierung durch die verschiedenen Abschnitte des Menüs zu ermöglichen, stellen Sie den Nutzer:innen eine leicht zugängliche Seite bereit, von der aus alle mit dem Datenschutz zusammenhängenden Handlungen (z. B. Einstellungen) und Informationen zugänglich sind. Diese Seite kann im Hauptnavigationsmenü des Anbieters, im Nutzerkonto, über die Datenschutzerklärung usw. zu finden sein.

Zusammengefasste Optionen: Zusammenfassung von Optionen, die denselben Verarbeitungszweck haben, sodass Nutzer:innen sie einfacher ändern können, dabei aber die Möglichkeit behalten, detailliertere Änderungen vorzunehmen. Wenn Social-Media-Plattformen zusammengefasste Optionen bieten, sollten diese keine unerwarteten oder nicht miteinander zusammenhängenden Elemente enthalten (z. B. Elemente mit unterschiedlichen Zwecken). Ist für die Verarbeitung eine Einwilligung erforderlich, müssen die zusammengefassten Optionen mit den EDSA-Leitlinien zur Einwilligung, insbesondere Rn. 42-44, im Einklang stehen.

Schnellzugriffe: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 29) (*werden Nutzer:innen beispielsweise über einen Aspekt der Verarbeitung informiert, werden sie gebeten, ihre diesbezüglichen Datenpräferenzen auf der entsprechenden Seite mit Einstellungen/auf dem Dashboard festzulegen*).

Selbsterklärende URL: Auf Seiten im Zusammenhang mit Datenschutzeinstellungen oder -informationen sollte eine Internetadresse verwendet werden, die deren Inhalt klar widerspiegelt. Beispielsweise könnte eine Seite, auf der die Kontrollfunktionen für den Datenschutz zentral zusammengefasst werden, eine URL wie [soziales-netzwerk.com]/datenschutzeinstellungen aufweisen.

Einheitliche Formulierungen: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 29).

Begriffsbestimmungen bereitstellen: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 29).

Verwendung von Beispielen: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 30).

Angeheftete Navigationsleiste: Eine Begriffsbestimmung ist im Anwendungsfall 2a zu finden (S. 36).

Benachrichtigungen: Eine Begriffsbestimmung ist im Anwendungsfall 2c zu finden (S. 42).

Folgen erläutern: Eine Begriffsbestimmung ist im Anwendungsfall 2c zu finden (S. 42).

Geräteübergreifende Einheitlichkeit: Eine Begriffsbestimmung ist im Anwendungsfall 3a zu finden (S. 51).

3.4 Richtig unterwegs in den sozialen Medien: Rechte betroffener Personen

Anwendungsfall 4: Wie man angemessene Anwendungen für die Ausübung der Rechte betroffener Personen bereitstellt

a. Beschreibung des Kontextes

142. Die Nutzung einer Social-Media-Plattform bedeutet, dass man deren Vorteile entsprechend den vom Anbieter angegebenen Zwecken in Anspruch nehmen kann. Für Nutzer:innen bedeutet dies auch, in der Lage zu sein, ihre Datenschutzrechte auszuüben. Diese Rechte sind Schlüsselemente des

Datenschutzes und der Kontrolle der eigenen Informationen, unabhängig davon, ob Daten von betroffenen Personen direkt und wissentlich bereitgestellt, von betroffenen Personen aufgrund der Nutzung des Dienstes oder des Geräts bereitgestellt oder aus der Analyse der von der betroffenen Person bereitgestellten Daten abgeleitet werden.⁶⁶ Aufgrund der Menge personenbezogener Daten, die auf der gesamten Plattform in Bewegung sind, muss es den Nutzer:innen möglich sein, ihre Daten mithilfe der in der DS-GVO vorgesehenen Rechte in klarer, intuitiver Weise zu kontrollieren. Der EDSA hat diese Grundsätze in mehreren Leitlinien erläutert.⁶⁷ Die Ausübung der Betroffenenrechte muss vom Beginn bis zum Ende der Nutzung der Plattform und in einigen Fällen auch dann noch möglich sein, wenn Nutzer:innen beschlossen haben, die Plattform zu verlassen, und der Verantwortliche ihre Daten noch nicht gelöscht hat. Auch Personen, die die Plattform nicht nutzen, müssen in die Lage versetzt werden, ihre Betroffenenrechte im Zusammenhang mit der Verarbeitung ihrer Daten auszuüben. Natürlich stehen je nach der Rechtsgrundlage für die Verarbeitung der Daten in einigen Fällen nicht alle Betroffenenrechte zur Verfügung. Der Social-Media-Anbieter sollte daher auch deutlich darlegen, warum bestimmte Rechte nicht gelten und warum einige von ihnen möglicherweise eingeschränkt sind. Wie bereits erwähnt und in den vorangegangenen Kapiteln dargelegt, muss die wirksame Ausübung der Betroffenenrechte sichergestellt werden. Zur Erleichterung der Ausübung von Betroffenenrechten sollten Automatisierung und andere Funktionen von Social-Media-Plattformen eingesetzt werden.

b. Maßgebliche Rechtsvorschriften

143. In der DS-GVO werden sieben verschiedene Betroffenenrechte beschrieben, die Betroffene unter bestimmten Voraussetzungen (z. B. Rechtsgrundlage der Verarbeitung usw.) ausüben können. Artikel 15 DS-GVO ermöglicht betroffenen Personen, Auskunft darüber zu erhalten, ob sie betreffende personenbezogene Daten verarbeitet werden und auf sie zuzugreifen, d. h. weitere Informationen über ihre Verarbeitung einzuholen, und eine Kopie dieser Daten zu erhalten. Artikel 16 DS-GVO enthält eine ausführliche Beschreibung des Rechts auf Berichtigung, das betroffenen Personen die Aktualisierung der vom Verantwortlichen verarbeiteten personenbezogenen Daten ermöglicht. Das Recht auf Löschung nach Artikel 17 DS-GVO ermöglicht betroffenen Personen, die Löschung der sie betreffenden personenbezogenen Daten zu erwirken. Das Recht auf Einschränkung der Verarbeitung nach Artikel 18 DS-GVO gibt den betroffenen Personen die Möglichkeit, die Verarbeitung ihrer personenbezogenen Daten vorübergehend einzustellen. Artikel 20 DS-GVO enthält das Recht auf Datenübertragbarkeit, das betroffenen Personen ermöglicht, ihre personenbezogenen Daten zu erhalten und einem anderen Verantwortlichen zu übermitteln.⁶⁸ Laut Artikel 21 DS-GVO haben betroffene Personen auch das Recht, Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten einzulegen. Und schließlich gewährt Artikel 22 DS-GVO betroffenen Personen das Recht, nicht

⁶⁶ Siehe Artikel-29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit gemäß der Verordnung 2016/679, WP242 rev.01, S. 10, <https://ec.europa.eu/newsroom/article29/items/611233/en>.

⁶⁷ Leitlinien zum Recht auf Datenübertragbarkeit und EDSA-Leitlinien 5/2019 zu den Kriterien des Rechts auf Vergessenwerden in Fällen in Bezug auf Suchmaschinen gemäß der DS-GVO (Teil 1) – nach öffentlicher Konsultation angenommene Version, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_de.

⁶⁸ Dieses Recht wird in den Leitlinien zum Recht auf Datenübertragbarkeit näher ausgeführt.

einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden.⁶⁹

144. Der EDSA betont, dass nicht alle diese Rechte für jede Social-Media-Plattform gelten, wobei dies von ihrer jeweiligen Rechtsgrundlage und den Zwecken der Verarbeitung personenbezogener Daten und der Art der erbrachten Dienste abhängt. Die Unterschiede sollten gemäß Artikel 12 DS-GVO vom Verantwortlichen erläutert werden. Dies bedeutet, dass die Informationen über die geltenden Rechte präzise und für die Nutzer:innen klar sein sollten und auch die Gründe dafür einschließen sollten, dass bestimmte Rechte nicht gelten. Eine solche Erklärung könnte den Umfang der Kommunikation mit den Nutzer:innen verringern, wenn diese versuchen, einige dieser Rechte auszuüben. Die Ausübung eines Rechts sollte gemäß Artikel 12 Absatz 2 DS-GVO einfach und zugänglich sein, und die Antwort sollte gemäß Artikel 12 Absatz 3 DS-GVO unverzüglich erfolgen. Ebenso sollte auf der Social-Media-Plattform erläutert werden, warum bestimmten Anträgen nicht entsprochen werden kann, und über die Möglichkeit informiert werden, gemäß Artikel 12 Absatz 4 DS-GVO bei einer benannten Aufsichtsbehörde Beschwerde einzulegen. Daher sind die folgenden irreführenden Gestaltungsmuster möglicherweise nicht auf alle oben genannten Rechte anwendbar. Das Recht auf Löschung wird im nächsten Kapitel ausführlich erörtert.

c. Irreführende Gestaltungsmuster

i. Inhaltsbezogene Muster

Behindern – Sackgasse (Anhang Checkliste 4.4.1)

145. Das irreführende Gestaltungsmuster **Sackgasse** kann sich unmittelbar auf den leichten Zugang zur Ausübung der Rechte auswirken. Wenn Links, die zur Ausübung eines Rechts weiterleiten, defekt sind oder wenn klare Erläuterungen zur Ausübung des Rechts fehlen, werden Nutzer:innen dieses Recht nicht ordnungsgemäß ausüben können, was gegen Artikel 12 Absatz 2 DS-GVO verstößt.

| |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Beispiel 44: Nutzer:innen klicken in den Datenschutzhinweisen auf „<i>Mein Auskunftsrecht ausüben</i>“, werden aber zu ihrem Profil weitergeleitet, das keine Funktionen im Zusammenhang mit der Ausübung des Rechts enthält.</p> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

146. Das oben genannte Beispiel eines irreführenden Gestaltungsmusters verdeutlicht das Erfordernis, den Nutzer:innen eine klare, intuitive Methode für die Ausübung ihrer Rechte nach Artikel 12 Absätze 1 und 2 DS-GVO zur Verfügung zu stellen, da sie diese andernfalls möglicherweise nicht ausüben können. Es reicht nicht aus, den Nutzer:innen zu bestätigen, dass sie über Betroffenenrechte gemäß Artikel 12 Absatz 1 DS-GVO (einschließlich der Art der Kommunikation) und insbesondere gemäß Artikel 13 Absatz 2 Buchstabe b und Artikel 14 Absatz 2 Buchstabe c DS-GVO verfügen. Die Nutzer:innen müssen auch in der Lage sein, die Rechte ohne Schwierigkeiten auszuüben, vorzugsweise in einer Weise, die in die Benutzeroberfläche der Plattform eingebettet ist, beispielsweise mittels Bereitstellung eines dazu bestimmten Formulars. Wenn Nutzer:innen erkennen, dass sich der Anbieter die Mühe gemacht hat, sich an die Erwartungen der Nutzer:innen bezüglich der rechtmäßigen Verarbeitung personenbezogener Daten und der Kontrolle über ihre Daten anzupassen, indem er die Ausübung von Rechten mit anderen Funktionen des Dienstes kombiniert, würde dies auch eine positivere Nutzererfahrung mit einer Plattform bedeuten. Wenn der Dienst der Social-Media-Plattform eine

⁶⁹ Siehe auch Artikel-29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, wp251rev.01, S. 19 ff., <https://ec.europa.eu/newsroom/article29/items/612053/en>.

Kommunikation in beide Richtungen zwischen den Nutzer:innen sowie zwischen dem Verantwortlichen und den Nutzer:innen ermöglicht, gibt es für den Verantwortlichen keinen Grund, seinen Kommunikationskanal zur Erleichterung von Anträgen betroffener Personen auf ein gesondertes Kommunikationsmittel wie E-Mail zu beschränken. Zugleich sollten betroffene Personen nicht gezwungen werden, zur Kommunikation mit dem Verantwortlichen die Plattform zu besuchen.⁷⁰ Darüber hinaus dürfen die Verantwortlichen dieses Recht betroffener Person nicht auf das Recht auf Kopie beschränken, sondern müssen stattdessen sicherstellen, dass sie den Nutzer:innen, die Auskunft über ihre Daten beantragen, auch die in Artikel 15 Absatz 1 DS-GVO genannten Informationen zur Verfügung stellen.⁷¹

Unbeständig – Sprachliche Diskontinuität (Anhang I Checkliste 4.5.4)

Beispiel 45: Beim Anklicken eines Links bezüglich der Ausübung der Rechte betroffener Personen werden die folgenden Informationen nicht in der/den Amtssprache(n) des Landes des Nutzers bereitgestellt, während dies bei dem Dienst selbst der Fall ist. Stattdessen werden die Nutzer:innen auf eine Seite in englischer Sprache weitergeleitet.

147. In Anbetracht des Grundsatzes der Transparenz nach Artikel 5 Absatz 1 Buchstabe a und Artikel 12 Absatz 1 DS-GVO müssen Nutzer:innen alle Informationen über ihre Rechte in klarer und verständlicher Weise erhalten. Dies muss sich auch auf den Standort der Nutzer:innen und die Sprache beziehen, die in dem Land oder Rechtssystem verwendet wird, in dem der Dienst angeboten wird. Die Tatsache, dass Nutzer:innen in irgendeiner Weise bestätigen, dass sie in der Lage sind, eine Fremdsprache zu verwenden, entbindet den Verantwortlichen nicht von seinen Pflichten. Das Gleiche gilt, wenn solche Fremdsprachenkenntnisse der Nutzer:innen aus ihren Tätigkeiten abgeleitet werden können. Die Informationen sollten für Nutzer:innen, die ihre Rechte ausüben, relevant und hilfreich sein.

Im Dunkeln gelassen – Mehrdeutige Formulierungen oder Informationen (Anhang I Checkliste 4.6.3)

148. Im Zusammenhang mit den Rechten betroffener Personen können Nutzer:innen, wie im folgenden Beispiel gezeigt wird, auch mit dem irreführenden Gestaltungsmuster ***Mehrdeutige Formulierungen oder Informationen*** konfrontiert werden.

Beispiel 46: In der Social-Media-Plattform wird nicht ausdrücklich darauf hingewiesen, dass Nutzer:innen in der EU das Recht haben, bei einer Aufsichtsbehörde Beschwerde einzulegen, sondern es wird lediglich darauf hingewiesen, dass es in einigen Ländern – ohne zu erwähnen, in welchen – Datenschutzbehörden gibt, mit denen der Anbieter bei Beschwerden zusammenarbeitet.

⁷⁰ Siehe EDSA-Leitlinien 1/2022 zu den Rechten der betroffenen Person – Auskunftsrecht, Rn. 136, Version 1.0, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access_de.

⁷¹ Siehe EDSA-Leitlinien 1/2022, Rn. 131, 142 und 145.

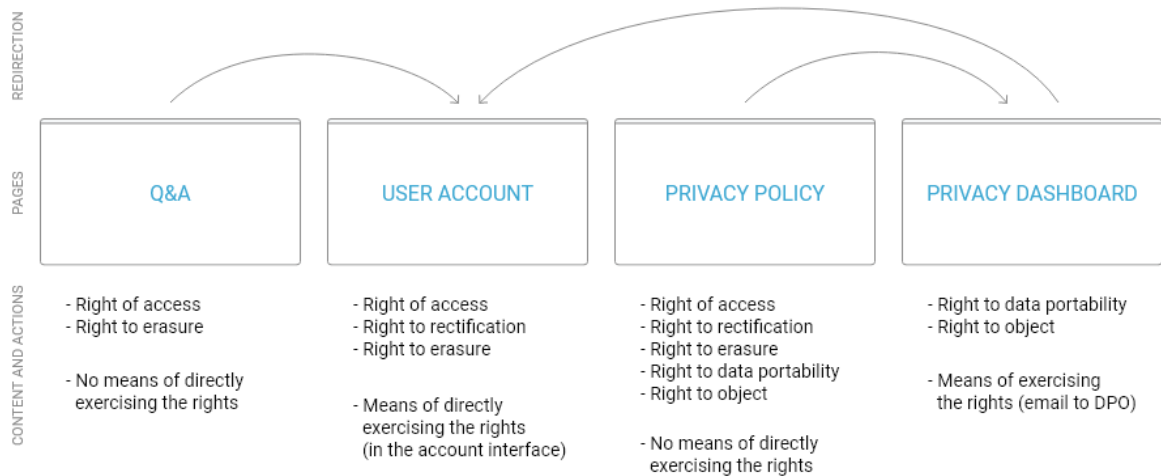
149. Social-Media-Anbieter müssen auch darauf achten, dass sie bei der Unterrichtung betroffener Personen über ihre Rechte das irreführende Gestaltungsmuster **Mehrdeutige Formulierungen oder Informationen** vermeiden. Nutzer:innen in einer Weise zu informieren, die in ihnen Unsicherheit darüber weckt, wie ihre Daten verarbeitet werden oder auf welche Weise sie eine gewisse Kontrolle über ihre Daten ausüben und somit ihre Rechte wahrnehmen können, verstößt gegen den Grundsatz der Transparenz. Darüber hinaus stellen vage Formulierungen keine präzise Sprache dar, wie sie in Artikel 12 Absatz 1 DS-GVO vorgeschrieben ist. Dadurch können die der betroffenen Person bereitgestellten Informationen unvollständig werden, was als Verstoß gegen Artikel 13 DS-GVO angesehen werden könnte. Das vorstehende Beispiel zeigt auch einen Verstoß gegen Artikel 13 Absatz 2 Buchstabe d DS-GVO, wonach die Verantwortlichen die betroffenen Personen über ihr Recht informieren müssen, bei einer Aufsichtsbehörde Beschwerde einzulegen. Im weiteren Sinne läuft dies auch Artikel 12 Absatz 2 DS-GVO zuwider, da der Anbieter die Ausübung des Beschwerderechts nicht erleichtert.

ii. Oberflächenbezogene Muster

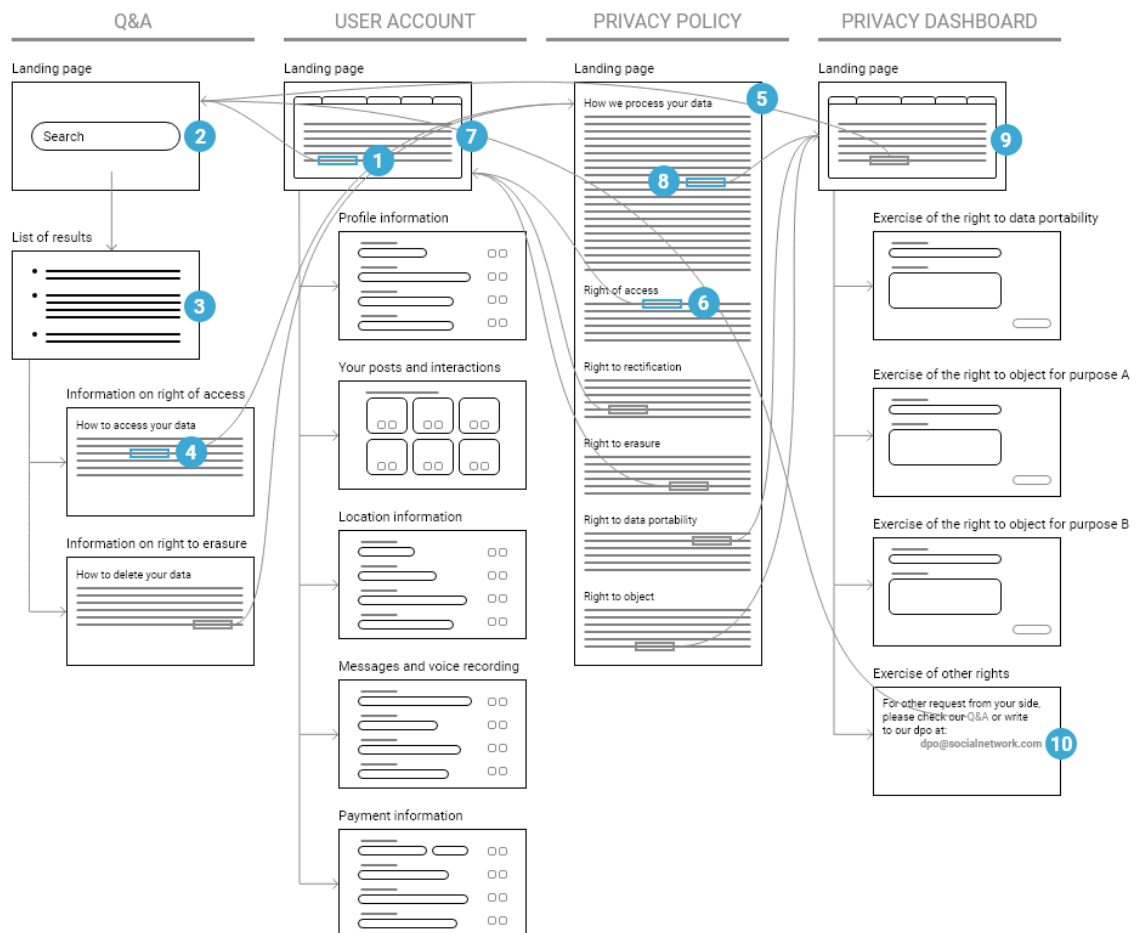
Überfrachtung – Datenschutz-Labyrinth (Anhang I Checkliste 4.1.2)

150. Wie bereits im Anwendungsfall 3b beschrieben, darf die Anzahl der für den Erhalt einschlägiger Datenschutzinformationen erforderlichen Schritte nicht übermäßig hoch sein. Dasselbe gilt für die Zahl der Schritte, mit denen die Rechte betroffener Personen durchgesetzt werden können.⁷² Nutzer:innen sollten folglich jederzeit in der Lage sein, die Website zur Ausübung von Rechten rasch zu erreichen, unabhängig davon, was ihr Ausgangspunkt war und wo auf der Social-Media-Plattform diese Funktion untergebracht ist. Social-Media-Anbieter sollten daher sorgfältig die unterschiedlichen Situationen erwägen, in denen Nutzer:innen eventuell ihre Rechte ausüben möchten, und den Zugang zu dem Ort, an dem sie dies tun können, entsprechend gestalten. Dies bedeutet, dass mehrere Pfade zur Erreichung eines Rechts betroffener Personen geschaffen und auf einer Plattform zur Verfügung gestellt werden können. Jeder Pfad sollte jedoch den Zugang zur Ausübung der Rechte erleichtern und keinen anderen Pfad stören. Ist dies nicht der Fall, wäre dies entgegen Artikel 12 Absatz 2 DS-GVO ein irreführendes Gestaltungsmuster des Typs **Datenschutz-Labyrinth** wie in den Beispielen 47 und 48 veranschaulicht.

⁷² Siehe oben, Rn. 123.



Beispiel 47: Hier stehen auf mindestens vier Seiten Informationen zu Datenschutzrechten zur Verfügung. Auch wenn in der Datenschutzerklärung über alle Rechte informiert wird, leitet sie nicht zu den entsprechenden Seiten für die einzelnen Rechte weiter. Hingegen finden die Nutzer:innen beim Besuch ihres Kontos über einige der Rechte, die sie ausüben können, gar keine Informationen. Dieses **Datenschutz-Labyrinth** zwingt Nutzer:innen dazu, zahlreiche Seiten zu durchforsten, um herauszufinden, wo sie die einzelnen Rechte ausüben können. Abhängig von ihrer Suche sind sie sich möglicherweise nicht aller Rechte bewusst, die sie besitzen.



Beispiel 48: In diesem Beispiel möchten die Nutzer:innen einige ihrer personenbezogenen Daten aktualisieren, finden aber in ihrem Konto keine Möglichkeit dazu. Sie klicken auf einen Link (1), der sie zur Seite „Fragen & Antworten“ weiterleitet, auf der sie ihre Frage (2) eingeben. Es erscheinen mehrere Ergebnisse (3), von denen einige mit den Auskunfts- und Lösungsrechten zusammenhängen. Nachdem sie alle Ergebnisse geprüft haben, klicken sie (4) auf den Link, der auf der Seite „Wie Sie auf Ihre Daten zugreifen können“ zur Verfügung steht. Er leitet sie zur Datenschutzerklärung (5) weiter. Dort finden sie Informationen über zusätzliche Rechte. Nachdem sie diese Informationen gelesen haben, klicken sie (6) auf den Link zur Ausübung des Rechts auf Berichtigung, der sie auf das Nutzerkonto weiterleitet (7). Unzufrieden kehren sie zur Datenschutzerklärung zurück und klicken den allgemeinen Link „Anfrage senden“ (8) an. Damit gelangen die Nutzer:innen zu ihrem Datenschutz-Dashboard (9). Da keine der verfügbaren Optionen ihrem Anliegen entspricht, gehen die Nutzer:innen schließlich auf die Seite „Ausübung anderer Rechte“ (10), auf der sie endlich eine Kontaktadresse finden.

151. Beide Beispiele veranschaulichen besonders langwierige und schwierige Wege zur Ausübung von Betroffenenrechten. Befinden sich die Mittel zur Ausübung verschiedener Betroffenenrechte nicht an

demselben Ort, sondern es steht eine Seite zur Verfügung, auf der alle Rechte betroffener Personen aufgeführt werden, sollte Letztere zu genau diesen unterschiedlichen Orten weiterleiten, nicht nur zu einem Ort oder einem Teil dieser Orte, wie in Beispiel 47 gezeigt. Das andere Beispiel zeigt ein Erlebnis, bei dem die Nutzer:innen nicht das Mittel finden, mit dem sie das gewünschte spezielle Recht, nämlich das Recht auf Berichtigung, einfach ausüben können. Denn an dem Ort, an dem dies gewöhnlich erfolgt, d. h. dem Nutzerkonto, wird das entsprechende Mittel nicht zur Verfügung gestellt. Bei der Suche nach einer anderen Möglichkeit zur Ausübung dieses Rechts können sie keine diesem besonderen Anliegen entsprechende Möglichkeit finden und müssen auf ein allgemeines Mittel im Datenschutz-Dashboard zurückgreifen.

152. Sind mehrere Pfade zur Ausübung eines Rechts angelegt worden, sollten Nutzer:innen stets ohne Schwierigkeiten einen Überblick über die Betroffenenrechte finden können. Datenschutzerklärungen sollten klar sein und könnten als Zugangstor zu den Seiten dienen, auf denen die Nutzer:innen ihre Rechte ausüben können. Dieses Dokument sollte alle geltenden Rechte enthalten. Sollte eines von ihnen aufgrund rechtlicher oder technischer Einschränkungen nicht zur Verfügung stehen, sollte dies ebenfalls erläutert werden, damit die Nutzer:innen ordnungsgemäß informiert werden. Es ist nicht nur für Nutzer:innen hilfreich, die Grenzen der Verarbeitungsvorgänge zu verstehen, die ihre Ursache entweder in ihrer Grundlage oder den von den Verantwortlichen getroffenen Vorkehrungen haben. Dies begrenzt ferner auch die Fälle, in denen ein Social-Media-Anbieter erklären muss, warum er einem von Nutzer:innen gestellten Antrag auf Ausübung eines Betroffenenrechts nicht nachkommen kann.

Aufwühlen – Vor aller Augen verborgen (Anhang I Checkliste 4.3.2)

153. Eine Beeinträchtigung der Fähigkeit der Nutzer:innen, den Ort zu erreichen, an dem sie ihr Recht ausüben können, kann auch dadurch eintreten, dass damit zusammenhängende Informationen oder Links mithilfe des irreführenden Gestaltungsmusters ***Vor aller Augen verborgen*** so gestaltet werden, dass sie kaum sichtbar sind.

Beispiel 49: Im Absatz unter dem Untertitel „Auskunftsrecht“ in der Datenschutzerklärung wird erläutert, dass die Nutzer:innen nach Artikel 15 Absatz 1 DS-GVO das Recht haben, Informationen zu erhalten. Dort wird jedoch nur die Möglichkeit der Nutzer:innen erwähnt, eine Kopie ihrer personenbezogenen Daten zu erhalten. Es ist kein direkter Link zur Ausübung dieser Komponente des Auskunftsrechts nach Artikel 15 Absatz 3 DS-GVO sichtbar. Vielmehr sind die ersten drei Wörter in dem Satz „Sie können eine Kopie Ihrer personenbezogenen Daten haben“ zart unterstrichen. Verharrt der Nutzer:innen mit seiner Maus über diesen Wörtern, wird ein kleiner Kasten mit einem Link zu den Einstellungen angezeigt.

154. Ergänzend zum vorhergehenden Abschnitt sollten alle Mittel, die der Verantwortliche für die Ausübung von Rechten bereitgestellt hat, leicht zugänglich sein. Diese Regel kann nicht hoch genug eingeschätzt werden. Eine Handlung des Verantwortlichen, wie sie oben beschrieben wird, kann nur als Versuch betrachtet werden, die Ausübung von Rechten durch die Nutzer:innen zu behindern, was gegen Artikel 12 Absatz 2 DS-GVO verstößt. Verantwortliche sollten eine solche Anfrage nicht behindern, unabhängig davon, was ihre Gründe sein mögen. Nach genauerer Prüfung durch eine Aufsichtsbehörde könnte dies in bestimmten Fällen zu einem Verstoß gegen die DS-GVO beitragen und somit zu Sanktionen gegen den Verantwortlichen führen.

Unbeständig – Uneinheitliche Schnittstelle (Anhang I Checkliste 4.5.3)

Beispiel 50: Die Social-Media-Plattform bietet verschiedene Versionen (Desktop, App, Browser für Mobilgeräte). In jeder Version werden die Einstellungen (die zur Auskunft/zum Widerspruch usw. führen) mit einem anderen Symbol angezeigt, sodass Nutzer:innen, die zwischen Versionen wechseln, verwirrt werden.

155. Sind Nutzer:innen mit Benutzeroberflächen für verschiedene Geräte konfrontiert, die dieselben Informationen durch unterschiedliche visuelle Symbole übermitteln, werden sie wahrscheinlich mehr Zeit benötigen oder Schwierigkeiten haben, Kontrollfunktionen, die sie von einem Gerät kennen, auf einem anderen zu finden. Im vorstehenden Beispiel ist dies darauf zurückzuführen, dass unterschiedliche Symbole oder Icons verwendet werden, um die Nutzer:innen zu den Einstellungen zu führen. Nutzer:innen auf solche Weise zu verwirren, könnte im Widerspruch zur Erleichterung der Betroffenenrechte nach Artikel 12 Absatz 2 DS-GVO stehen.

Behindern – Länger als erforderlich (Anhang I Checkliste 4.4.2)

156. Schließlich kann jeder Versuch, die Ausübung eines Rechts ***länger als erforderlich*** zu gestalten, als mit der DS-GVO unvereinbar angesehen werden.

Beispiel 51: Möchten Nutzer:innen den Namen und den Ort ihrer Schule oder den Verweis auf eine Veranstaltung, an der sie teilgenommen und geteilt haben, löschen, öffnet sich ein zweites Fenster, in dem sie gebeten werden, diese Entscheidung zu bestätigen („*Möchten Sie dies wirklich tun? Warum möchten Sie dies tun?*“).

157. Ähnlich wie bei der Anzahl der Ebenen in einer Datenschutzerklärung (Anwendungsfall 2a) und der Anzahl der Schritte, um eine Einstellung zu erreichen oder zu ändern (Anwendungsfall 3b), sollte auch die Zahl der Schritte oder Klicks, die Nutzer:innen unternehmen müssen, um ein Recht auszuüben, nicht übermäßig hoch sein. Dies hängt natürlich von der Komplexität der vom Verantwortlichen durchgeführten Vorgänge ab, wobei der jeweilige Kontext zu berücksichtigen ist. Es wäre jedoch unangemessen, von den Nutzer:innen zu verlangen, dass sie zur Ausübung ihrer Rechte eine große Zahl unnötiger Handlungen unternehmen. Beispielsweise sollten Nutzer:innen nicht durch zusätzliche Fragen, etwa ob sie dieses Recht tatsächlich ausüben möchten oder was die Gründe für einen solchen Antrag sind, entmutigt werden. In den meisten Fällen sollten sie in der Lage sein, ihr Recht auf einfache Weise auszuüben, ohne dass ihre Motivation infrage gestellt wird. Derartige, im vorstehenden Beispiel veranschaulichte Praktiken können als Verstoß gegen Artikel 12 Absatz 2 DS-GVO angesehen werden, da der Verantwortliche die Ausübung der Rechte mit unnötigen Schritten behindert. Dies schließt natürlich nicht aus, dass der Verantwortliche Rückmeldungen erhält, wenn er anschließend mit dem Ziel, den Dienst zu verbessern, zusätzliche Fragen stellt. Indem diese Frage im Nachhinein gestellt wird, hängt ihre Beantwortung allein vom Willen der Nutzer:innen ab und wird nicht irrtümlich für eine Voraussetzung für die Ausübung eines Rechts gehalten.

d. Best Practices

Formular für die Ausübung der Rechte: Um den Nutzer:innen die Wahrnehmung ihrer Rechte aus der DS-GVO zu erleichtern, sollte ein spezielles Formular bereitgestellt werden, das die Nutzer:innen beim Verständnis ihrer Rechte unterstützt und ihnen bei dieser Art von Anfragen Orientierungshilfe bietet.

Schnellzugriffe: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 29) (z. B. *Bereitstellung eines Links zur Löschung des Kontos im Nutzerkonto*).

Einheitliche Formulierungen: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 29).

Begriffsbestimmungen bereitstellen: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 29).

Verwendung von Beispielen: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 30).

Angeheftete Navigationsleiste: Eine Begriffsbestimmung ist im Anwendungsfall 2a zu finden (S. 36).

Folgen erläutern: Eine Begriffsbestimmung ist im Anwendungsfall 2c zu finden (S. 42).

Geräteübergreifende Einheitlichkeit: Eine Begriffsbestimmung ist im Anwendungsfall 3a zu finden (S. 51).

Datenschutzverzeichnis: Eine Begriffsbestimmung ist im Anwendungsfall 3b zu finden (S. 59).

Relation der Datenschutzkontrollfunktionen: Eine Begriffsbestimmung ist im Anwendungsfall 3b zu finden (S. 45).

3.5 Tschüss und Auf Wiedersehen: Ein Nutzerkonto in sozialen Medien verlassen

Anwendungsfall 5: Vorübergehendes Pausieren des Kontos/Löschung aller personenbezogenen Daten

a. Beschreibung des Kontextes und maßgebliche Rechtsvorschriften

158. Das Ende des Lebenszyklus eines Kontos beschreibt die Situation, in der Nutzer:innen beschließen, das soziale Netzwerk zu verlassen. In dieser Situation beschließen die Nutzer:innen in der Regel, die Social-Media-Plattform dauerhaft zu verlassen. Häufig besteht jedoch auch die Möglichkeit, das Konto nur vorübergehend zu deaktivieren und den Dienst zu pausieren. Die rechtlichen Folgen beider Entscheidungen sind unterschiedlich und werden im Folgenden beschrieben.

i. Dauerhafte Löschung des Kontos

159. Die Entscheidung, die Social-Media-Plattform dauerhaft zu verlassen, geht mit dem Recht auf Löschung nach Artikel 17 Absatz 1 Buchstabe a DS-GVO einher.
160. Der Begriff „Löschung“ wird in Artikel 17 DS-GVO nicht rechtlich definiert und wird nur in Artikel 4 Nummer 2 DS-GVO als Form der Verarbeitung genannt. Löschung kann allgemein so verstanden werden, dass es (tatsächlich) unmöglich ist, die zuvor in den zu löschenden Daten enthaltenen Informationen über eine betroffene Person zu erkennen. Nach der Löschung darf es niemandem mehr möglich sein, die fraglichen Informationen ohne unverhältnismäßigen Aufwand zu erkennen.
161. Anonymisierung ist eine weitere Möglichkeit, die Beziehung zu einer Person dauerhaft zu beseitigen. Mit anderen Worten soll der Einsatz von Anonymisierungstechniken sicherstellen, dass die betroffene Person nicht mehr identifiziert werden kann. Anonymisierung bedeutet auch, dass die datenschutzrechtlichen Grundsätze – wie der Grundsatz der Zweckbindung – nicht mehr anwendbar sind (siehe Erwägungsgrund 26 Sätze 4 und 5).
162. Nach Artikel 12 Absatz 2 DS-GVO muss der Verantwortliche der betroffenen Person die Ausübung ihrer Rechte gemäß den Artikeln 15 bis 22 erleichtern. Danach dürfen bei der Geltendmachung der Rechte betroffener Personen keine wesentlichen oder formellen Hürden geschaffen werden. Wenn also die Ausübung des Rechts auf Löschung ohne konkreten Grund erschwert wird, stellt dies einen Verstoß gegen die DS-GVO dar. Zwar gibt es einen triftigen Grund dafür, dass Social-Media-Anbieter die Folgen, wie die Löschung sämtlicher personenbezogener Daten, objektiv erläutern und dass sie die betroffenen Personen auffordern, diese Entscheidung zu bestätigen,⁷³ doch müssen auch in diesem Anwendungsfall unnötige Hürden vermieden werden. Daraus folgt beispielsweise, dass eine eventuelle Bedenkzeit zwischen den Anträgen der Nutzer:innen auf Löschung von Konten und der tatsächlichen Löschung des Kontos verhältnismäßig sein muss. Eine solche Frist darf folglich unter Berücksichtigung der notwendigen technischen Gründe für Verzögerungen bei der sofortigen Löschung sowie einer kurzen Frist für die (erneute) Prüfung der Löschung seitens der Nutzer:innen, sobald sie den Vorgang zur Löschung des Kontos ausgelöst haben, nicht übermäßig lang sein. Der freie Wille der Nutzer:innen, ihre Meinung zu ändern, muss zwar geachtet werden, jedoch dürfen die Anbieter nicht versuchen, einen solchen Meinungswechsel auszulösen, indem sie die Nutzer:innen zur Rückkehr anregen, was zudem eine Beschränkung des Rechts der Nutzer:innen auf Löschung darstellen würde. Während der Bedenkzeit könnte der Löschvorgang in manchen Fällen unterbrochen werden, z. B. wenn sich der Nutzer:innen erneut einloggt. Kann die Löschung nicht abgeschlossen werden, muss

⁷³ Im Gegensatz zu den anderen Rechten betroffener Personen, siehe Rn. 154.

der Nutzer:innen darüber informiert werden und Anweisungen erhalten, wie die Löschung abgeschlossen werden kann.

163. Die Entscheidung, die Social-Media-Plattform zu verlassen, zieht die Folgen der Löschung gemäß Artikel 17 Absatz 1 DS-GVO nach sich. Beantragt eine betroffene Person die Löschung des jeweiligen Kontos, muss der Verantwortliche einer Plattform die Daten löschen. Dennoch können einige Daten über einen bestimmten Zeitraum auf der Plattform verbleiben, wenn Artikel 17 Absatz 3 DS-GVO anwendbar ist. Die in Artikel 17 Absatz 3 der DS-GVO aufgeführten Ausnahmen sind eng auszulegen und gelten nur in den in diesem Teil der Vorschrift ausdrücklich genannten Fällen. Jede Ausnahme, auf die sich ein Verantwortlicher nach Artikel 17 Absatz 3 DS-GVO beruft, und die entsprechende Speicherung von Daten muss vom Verantwortlichen begründet werden, z. B. wenn der Verantwortliche nach nationalem Recht verpflichtet ist, Informationen über die betroffene Person aus zwingenden Gründen des öffentlichen Interesses, zur Ausübung des Rechts auf freie Meinungsäußerung und Information oder aus steuerlichen Gründen zu speichern. Es versteht sich von selbst, dass solche verbleibenden Daten nur intern vom Anbieter gespeichert werden und für andere Nutzer:innen nicht öffentlich sichtbar sein sollten. Eine Ausnahme nach Artikel 17 Absatz 3 DS-GVO ermöglicht es dem Anbieter jedoch keineswegs, das Konto der betroffenen Person länger zu führen, als von den Nutzer:innen nach ihrer Löschungsanfrage beabsichtigt.
164. Unabhängig von einem Antrag auf Löschung des Kontos darf in Fällen, in denen Nutzer:innen ihre Einwilligung nach Artikel 7 Absatz 3 DS-GVO widerrufen, eine Verarbeitung ihrer auf Einwilligungsbasis übermittelten Daten gemäß Artikel 6 Absatz 1 Buchstabe a DS-GVO nicht mehr erfolgen. Andere Verarbeitungsvorgänge, bei denen sich der Social-Media-Anbieter auf andere Rechtsgrundlagen aus Artikel 6 Absatz 1 DS-GVO stützt, können in diesem Fall unter bestimmten Umständen noch stattfinden.
165. Wenn Nutzer:innen jedoch um Löschung ihres Kontos bitten, sollte unabhängig von der zugrunde liegenden Rechtsgrundlage keine weitere Verarbeitung erfolgen, es sei denn, eine der in Artikel 17 Absatz 3 DS-GVO abschließend aufgeführten Ausnahmen findet Anwendung. In diesem Zusammenhang ist unbedingt zu bedenken, dass die Speicherung auf den vorstehend genannten Mindestumfang zu beschränken ist.
166. Nach Artikel 25 Absatz 1 DS-GVO trifft der Verantwortliche geeignete technische und organisatorische Maßnahmen zur praktischen Umsetzung der Datenschutzgrundsätze. Nach den Leitlinien 4/2019 zu Artikel 25 - Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen können als technische und organisatorische Maßnahmen im weiteren Sinne alle Methoden oder Mittel verstanden werden, die ein Verantwortlicher bei der Verarbeitung anwenden kann. Dass Maßnahmen geeignet sind, bedeutet, dass sie dazu dienen können, den beabsichtigten Zweck zu erreichen, d. h. sie müssen die Datenschutzgrundsätze wirksam umsetzen. Das Erfordernis der Eignung steht daher in engem Zusammenhang mit dem Erfordernis der Wirksamkeit.⁷⁴

⁷⁴ Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Seite 7, Rn. 8.

ii. Vorübergehendes Pausieren des Kontos

167. Alternativ erhalten die Nutzer:innen die Möglichkeit, ihr Konto vorübergehend zu pausieren, sodass sie die sozialen Medien für einen bestimmten Zeitraum verlassen können, ohne ihr Konto dauerhaft zu löschen. In diesem Fall wird das Konto vorübergehend deaktiviert, und das Profil, die Bilder, Kommentare und Reaktionen werden verborgen, bis die Nutzer:innen ihr Konto reaktivieren, indem sie sich beispielsweise erneut einloggen. Der Hauptunterschied zur Löschung besteht darin, dass die personenbezogenen Daten im sozialen Netzwerk verbleiben und das Konto von Nutzer:innen ohne neue Registrierung wieder aktiviert werden kann.
168. Nutzer:innen, die den Vorgang der Kontolöschung einleiten, stellen eventuell fest, dass die Option, das Konto stattdessen vorübergehend zu pausieren, vorab ausgewählt wurde. Es könnte zwar nützlich sein, dass Nutzer:innen, die ihr Konto nicht dauerhaft löschen möchten, eine Option zum vorübergehenden Pausieren angeboten wird. Jedoch dürfen Social-Media-Anbieter den Nutzer:innen solche Übergangszeiträume nicht vorschreiben, insbesondere nicht mittels Vorauswahl. Durch das Angebot der Möglichkeit zur Deaktivierung weckt der Anbieter bei den Nutzer:innen berechnete Erwartungen, dass ihre personenbezogenen Daten nicht in der gleichen Weise verarbeitet werden wie während der aktiven Nutzung des Kontos und dass der Anbieter die Verarbeitung personenbezogener Daten in diesem Zeitraum auf das absolut notwendige Maß beschränkt. Nutzer:innen könnten erwarten, dass ihre Daten für bestimmte Zwecke nicht oder nicht vollständig verarbeitet werden, z. B. durch die Verbesserung ihres Profils durch Besuche auf Webseiten Dritter, die geeignete Tools für die gezielte Ansprache oder Tracking verwenden. Neben der transparenten Information der Nutzer:innen über die Folgen der vorübergehenden Aussetzung ihres Kontos muss jede Verarbeitung von Daten, die während dieser Pausenzeit stattfindet, auf einer gültigen Rechtsgrundlage beruhen.
169. Im Hinblick auf Datenverarbeitungen, die sich gemäß Artikel 6 Absatz 1 Buchstabe a DS-GVO auf eine Einwilligung stützen, muss der Social-Media-Anbieter berücksichtigen, dass die Nutzer:innen erwarten, dass sich die Einwilligung, die sie während der Registrierung oder danach erteilen, nur auf die Datenverarbeitung während ihrer aktiven Nutzung des Kontos erstreckt. Der EDSA erkennt an, dass die Dauer der Einwilligung vom Kontext, vom Umfang der ursprünglichen Einwilligung und von den Erwartungen der betroffenen Person abhängt.⁷⁵ Obwohl es in der DS-GVO keine spezielle Frist für die Dauer der Einwilligung gibt, hängt die Gültigkeit vom Kontext, vom Umfang der ursprünglichen Einwilligung und von den Erwartungen der betroffenen Person ab.⁷⁶ Wenn sich die Verarbeitungsvorgänge beträchtlich ändern oder weiterentwickeln, ist die ursprüngliche Einwilligung nicht länger gültig.⁷⁷ Der EDSA empfiehlt als Best Practice, die Einwilligung in angemessenen Zeitabständen zu erneuern.⁷⁸ Alle Informationen erneut zur Verfügung zu stellen, hilft dabei, sicherzustellen, dass die betroffenen Personen gut darüber informiert bleiben, wie ihre Daten verwendet werden und wie sie ihre Rechte ausüben können.⁷⁹ Ist dies der Fall, muss die Einwilligung erneut eingeholt werden⁸⁰ und alle entsprechenden Anforderungen müssen erfüllt sein.
170. Die vernünftigen Erwartungen der betroffenen Person sollten ebenfalls berücksichtigt werden, wenn Artikel 6 Absatz 1 Buchstabe f DS-GVO anwendbar ist (siehe Erwägungsgrund 47). Insbesondere ist zu prüfen, ob die betroffene Person zum Zeitpunkt und im Zusammenhang mit der Erhebung der personenbezogenen Daten vernünftigerweise erwarten kann, dass eine Verarbeitung zu diesem Zweck

⁷⁵ Leitlinien 5/2020 zur Einwilligung, Rn. 110.

⁷⁶ Leitlinien 5/2020 zur Einwilligung, Rn. 110.

⁷⁷ Leitlinien 5/2020 zur Einwilligung, Rn. 110.

⁷⁸ Leitlinien 5/2020 zur Einwilligung, Rn. 111.

⁷⁹ Leitlinien 5/2020 zur Einwilligung, Rn. 111.

⁸⁰ Siehe Leitlinien 5/2020 zur Einwilligung, Rn. 110.

möglicherweise stattfindet. Die Nutzer:innen erwarten jedoch vernünftigerweise, dass während der Deaktivierung nur erforderliche Datenverarbeitungen stattfinden. Darüber hinaus kann sich der Anbieter nur dann auf ein berechtigtes Interesse berufen, wenn alle Schritte der Prüfung des berechtigten Interesses, einschließlich der Abwägung, erfüllt sind. Jedes überwiegende Interesse bzw. alle Grundrechte und Grundfreiheiten der betroffenen Person sind im Rahmen einer Einzelfallprüfung zu bewerten.

171. Da vertragliche Verpflichtungen während der Deaktivierung ebenfalls weitgehend ausgesetzt werden, sind Datenverarbeitungsvorgänge gemäß Artikel 6 Absatz 1 Buchstabe b DS-GVO nur in begrenztem Umfang erforderlich. Nur die Speicherung der Daten der Nutzer:innen bis zur endgültigen Entscheidung über die Reaktivierung oder Löschung kann als erforderlich angesehen werden.
172. Da alle früheren Datenverarbeitungen auf ein aktives Konto abzielten, müssen zusätzliche Informationen über die Verarbeitung während der Deaktivierung bereitgestellt werden, wenn sie nicht in den allgemeinen Informationen nach den Artikeln 13 und 14 DS-GVO enthalten sind. Dies ergibt sich aus den Grundsätzen der Transparenz und der Verarbeitung nach Treu und Glauben gemäß Artikel 5 Absatz 1 Buchstabe a DS-GVO und der Zweckbindung aus Artikel 5 Absatz 1 Buchstabe b DS-GVO. Die Datenverarbeitung nach der Deaktivierung muss mit einer ausreichenden Unterrichtung der betroffenen Person einhergehen. Daher muss der Social-Media-Anbieter die Nutzer:innen während der Pausenzeit umfassend über die tatsächliche Verarbeitung und ihre Zwecke informieren und erforderlichenfalls eine neue Einwilligung einholen.

b. Irreführende Gestaltungsmuster

i. Inhaltsbezogene Muster

Überfrachtung – Datenschutz-Labyrinth (Anhang I Checkliste 4.1.2)

173. In diesem Anwendungsfall tritt das irreführende Gestaltungsmuster ***Datenschutz-Labyrinth*** ein, wenn Nutzer:innen unter Massen von auf mehrere Orte verteilten Informationen begraben werden, um sie, wie das nachstehende Beispiel zeigt, von der Löschung ihres Kontos abzuhalten. Einige zusätzliche Informationen vor diesem Schritt sind zwar recht wünschenswert, z. B. die Angabe, dass die Nutzer:innen vor der Löschung Zugang zu ihren Daten haben. Jedoch sind allgemeine, damit nicht zusammenhängende Informationen, nicht mehr von entscheidender Bedeutung. Nutzer:innen sollten bei diesem Schritt nicht unnötig aufgehalten werden.

Beispiel 52: Nutzer:innen suchen nach dem Recht auf Löschung. Sie müssen die Kontoeinstellungen aufrufen, ein Untermenü namens „Privatsphäre“ öffnen und ganz nach unten scrollen, um einen Link zur Löschung des Kontos zu finden.

Aufwühlen – Emotionale Steuerung (Anhang I Checkliste 4.3.1)

Beispiel 53: Auf der ersten Informationsebene erhalten die Nutzer:innen Informationen, in denen nur die negativen Folgen der Löschung ihrer Konten betont werden (z. B. „*Sie werden alles für immer verlieren*“ oder „*Ihre Freunde werden Sie vergessen*“).

174. Während es gesellschaftlich angemessen erscheint, die Beendigung des Vertragsverhältnisses zu bedauern, und dies folglich rechtlich schwer zu erfassen ist, stellt eine umfassende Beschreibung der vermeintlich negativen Folgen, die Nutzer:innen durch die Löschung ihres Kontos entstehen, ein

Hindernis für ihre Entscheidung dar, wenn dies wie im vorstehenden Beispiel dargestellt geschieht, das mit der Angst, etwas zu verpassen, spielt und die Entscheidung zur Löschung des Kontos besonders strapaziös erscheint. Eine solche **Emotionale Steuerung**, die den Nutzer:innen damit droht, dass sie bei der Löschung ihres Kontos allein zurück gelassen werden, stellt einen Verstoß gegen die Verpflichtung zur Erleichterung der Ausübung der Rechte betroffener Personen nach Artikel 12 Absatz 2 DS-GVO sowie gegen den Grundsatz von Treu und Glauben nach Artikel 5 Absatz 1 Buchstabe a DS-GVO dar.

Im Dunkeln gelassen – Mehrdeutige Formulierungen oder Informationen (Anhang I Checkliste 4.6.3)

175. Im Zusammenhang mit der Löschung eines Nutzerkontos können Nutzer:innen auch mit dem irreführenden Gestaltungsmuster **Mehrdeutige Formulierungen oder Informationen** konfrontiert werden, wie das folgende Beispiel zeigt.

Beispiel 54: Wenn Nutzer:innen ihr Konto löschen, erhalten sie keine Informationen über die Dauer für die ihre Daten nach der Löschung des Kontos gespeichert werden. Schlimmer noch: Die Nutzer:innen werden Nutzer:innenan keinem Punkt des gesamten Löschvorgangs auf die Tatsache hingewiesen, dass „*einige der personenbezogenen Daten*“ auch nach der Löschung eines Kontos gespeichert werden könnten. Sie müssen die Informationen quer durch die verschiedenen verfügbaren Informationsquellen selbst suchen.

Beispiel 55: Nutzer:innen können ihr Konto nur über in ihrem Konto verfügbare Links mit der Bezeichnung „*Tschüss*“ oder „*Deaktivieren*“ löschen.

176. In diesen Beispielen lässt die für die Links verwendete Formulierung nicht eindeutig erkennen, dass die Nutzer:innen zum Vorgang der Kontolöschung weitergeleitet werden. Stattdessen werden die Nutzer:innen wahrscheinlich andere Funktionen wie das Ausloggen bis zur nächsten Nutzung oder die Deaktivierung ihres Kontos vermuten. Dies könnte für sich genommen als Verstoß gegen Artikel 12 Absatz 2 DS-GVO ausgelegt werden, wonach die Verantwortlichen die Ausübung der Rechte von betroffenen Personen erleichtern sollten. Da die Social-Media-Plattform hinsichtlich der Erwartungen der Nutzer:innen im Zusammenhang mit dem Link Verwirrung schafft, erleichtert sie die Ausübung des Rechts auf Löschung nicht in vollem Umfang. Die Verwendung solcher mehrdeutigen Wörter in anderen Zusammenhängen könnte gegen Bestimmungen der DS-GVO wie Artikel 7 DS-GVO und im weiteren Sinne auch gegen Artikel 17 Absatz 1 Buchstabe b DS-GVO verstoßen.

ii. Oberflächenbezogene Muster

Überspringen – Trügerische Bequemlichkeit (Anhang I Checkliste 4.2.1)

Beispiel 56: Bei der Löschung ihres Kontos erhalten die Nutzer:innen zwei Optionen, zwischen denen sie wählen können: Ihr Konto zu löschen oder vorübergehend zu pausieren. Standardmäßig ist die Option zum vorübergehenden Pausieren vorausgewählt.

177. Die erste Option, also das Konto zu löschen, führt zur Löschung aller personenbezogenen Daten von Nutzer:innen, was bedeutet, dass die Social-Media-Plattform nicht mehr im Besitz dieser Daten ist, wobei Daten ausgenommen sind, die unter die vorübergehende Ausnahme nach Artikel 17 Absatz 3

DS-GVO fallen. Im Gegensatz dazu werden bei der zweiten Option, also dem vorübergehenden Pausieren des Kontos, alle personenbezogenen Daten gespeichert und potenziell vom Anbieter verarbeitet. Dies birgt zwangsläufig mehr Risiken für die betroffene Person, wenn es beispielsweise zu einer Datenpanne kommt und auf die vom Anbieter noch gespeicherten Daten zugegriffen wird und sie vervielfältigt, übertragen oder auf andere Weise verarbeitet werden. Die Vorauswahl der Option einer vorübergehenden Aussetzung dürfte die Nutzer:innen dazu veranlassen, diese Option auszuwählen, statt ihr Konto wie ursprünglich vorgesehen zu löschen. Daher kann die in diesem Beispiel beschriebene Praxis als Verstoß gegen Artikel 12 Absatz 2 DS-GVO angesehen werden, da sie in diesem Fall die Ausübung des Rechts auf Löschung nicht erleichtert und sogar versucht, Nutzer:innen davon abzubringen.

Überspringen – „Schau, dort drüben“ (Anhang I Checkliste 4.2.2)

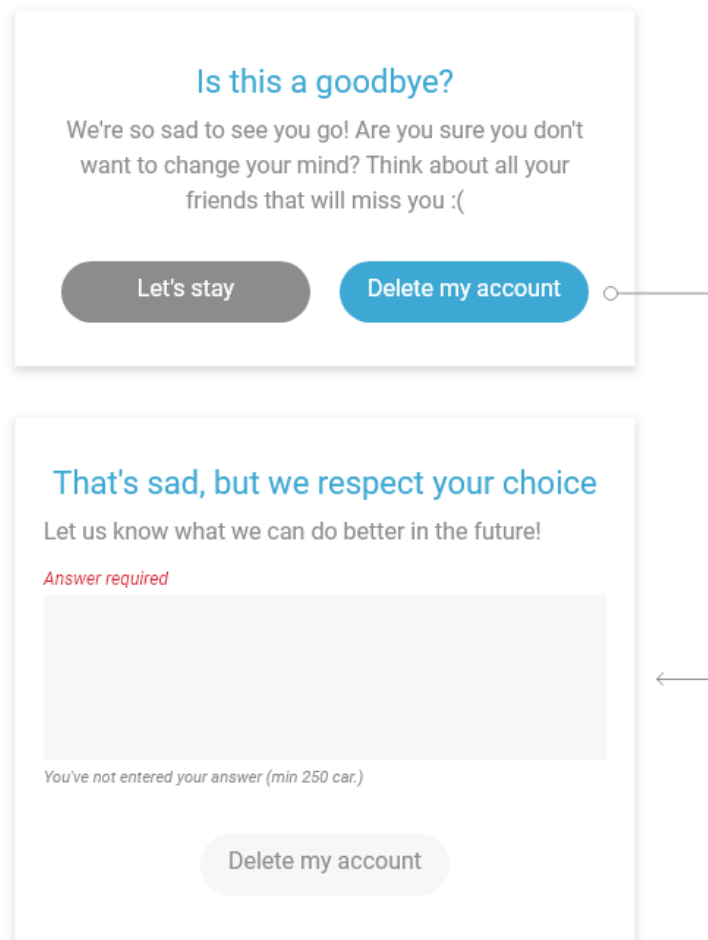
178. Nutzer:innen ein Mittel zum Herunterladen ihrer Daten zur Verfügung zu stellen, wenn sie ihren Wunsch zur Löschung ihres Kontos signalisieren, kann eine relevante Option darstellen. Tatsächlich werden ihre personenbezogenen Daten nach einem bestimmten Zeitraum gelöscht, sobald das Konto gelöscht worden ist. Dies bedeutet, dass sie ihre personenbezogenen Daten vollständig verlieren werden, wenn sie keine Kopie davon erhalten. Die Darstellung dieser Option kann jedoch, wie das folgende Beispiel zeigt, ein irreführendes Gestaltungsmuster des Typs „**Schau, dort drüben**“ sein.

Beispiel 57: Nachdem sie „Mein Konto löschen“ angeklickt haben, wird den Nutzer:innen vor dem Löschen des Kontos die Option vorgestellt, ihre Daten herunterzuladen. Und zwar implementiert als Recht auf Datenübertragbarkeit. Klicken sie die Option zum Herunterladen ihrer Informationen an, werden die Nutzer:innen auf eine Download-Informationsseite weitergeleitet. Sobald die Nutzer:innen jedoch entschieden haben, was sie herunterladen wollen und wie sie dies tun möchten, werden sie nicht zum Löschvorgang zurückgeleitet.

179. Im vorstehenden Beispiel könnte davon ausgegangen werden, dass die Art und Weise, wie die Download-Option eingesetzt wird, die Ausübung des Rechts auf Löschung bezogen auf die Löschung des Kontos nicht erleichtert. Wenn Nutzer:innen ihre Daten heruntergeladen haben, werden sie nicht wieder zum Löschvorgang zurückgeleitet. Die Rückkehr dorthin erfordert mehrere Klicks. Eine solche Behinderung der Ausübung eines Rechts verstößt gegen Artikel 12 Absatz 2 DS-GVO. Darüber hinaus ist die Bereitstellung eines Mittels, mit dem der Löschvorgang nach dem Herunterladen der Daten leicht erreicht werden kann, eine einfach zu implementierende Funktion. In dieser Hinsicht könnte anzunehmen sein, dass die Verpflichtung zur Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Artikel 25 Absatz 1 DS-GVO nicht erfüllt wird, da die Nutzer:innen ihre Rechte nicht wirksam ausüben können.

Behindern – Länger als erforderlich (Anhang I Checkliste 4.4.2)

180. Wie in Anwendungsfall 4 dargelegt, könnten irrelevante Schritte, die der Ausübung eines Rechts hinzugefügt werden, gegen Bestimmungen der DS-GVO verstoßen, insbesondere gegen Artikel 12 Absatz 2. Dies gilt für den Zeitpunkt, an dem Nutzer:innen beabsichtigen, ihr Konto zu löschen, da dies das Recht auf Löschung im Zusammenhang mit einem solchen Antrag beeinträchtigen würde.



Beispiel 58: In diesem Beispiel sehen die Nutzer:innen, nachdem sie auf den entsprechenden Link oder die entsprechende Schaltfläche in ihrem Konto geklickt haben, zunächst ein Bestätigungsfeld für die Löschung ihres Kontos. Auch wenn in dem Bestätigungsfeld eine gewisse **Emotionale Steuerung** vorliegt, kann dieser Schritt als Sicherheitsmaßnahme betrachtet werden, damit die Nutzer:innen ihr Konto nicht nach einem falschen Klick in ihrem Konto löschen können. Wenn Sie jedoch auf die Schaltfläche „Mein Konto löschen“ klicken, werden sie mit einem zweiten Kästchen konfrontiert, in dem sie aufgefordert werden, den Grund für das Verlassen des Kontos in Textform zu beschreiben. Bevor sie keine Eingabe in dem Feld vorgenommen haben, können sie ihr Konto nicht löschen, da die mit dieser Handlung verbundene Schaltfläche inaktiv und „ausgegraut“ ist. Diese Praxis gestaltet die Löschung eines Kontos **länger als erforderlich**, insbesondere weil die Aufforderung an die Nutzer:innen, einen Text mit der Beschreibung der Gründe zu erstellen, aus denen sie ein Konto verlassen wollen, zusätzlichen Arbeits- und Zeitaufwand erfordert und für die Löschung des Kontos nicht verpflichtend sein sollte.

181. Wie bereits erwähnt wurde, sollten Nutzer:innen bei der Ausübung eines Rechts keine Fragen beantworten müssen, die nicht mit der Ausübung des Rechts selbst in Zusammenhang stehen. Seine Wahl begründen oder erläutern zu müssen, wie die Social-Media-Plattform verbessert werden sollte,

fällt nicht in diese Kategorie. In dem dargestellten Beispiel wird dieses Problem noch verschärft, da betroffene Personen, statt einen vorgefertigten Vorschlag in einer Liste auszuwählen, eine Antwort schreiben müssen, was für sie sogar noch belastender ist, da sie eine vollständige Antwort erstellen müssen. Ein solcher Mechanismus könnte einige Nutzer:innen von der Ausübung ihres Rechts vollständig ausschließen, wenn sie sich nicht wohl dabei fühlen, eine Antwort auszuformulieren.

182. Dies bedeutet jedoch nicht, dass eine Liste vorgefertigter Antworten ein akzeptabler Schritt ist, mit dem das Verfahren zur Löschung des eigenen Kontos ergänzt werden kann. Dies trifft insbesondere dann zu, wenn diese Antworten mit weiteren Schritten und Handlungen verbunden sind, die von den Nutzer:innen verlangt werden, wie das nachstehende Beispiel zeigt.

Beispiel 59: Der Anbieter schreibt den Nutzer:innen zwingend vor, eine Frage zu den Gründen für die Löschung ihres Kontos zu beantworten, indem sie Antworten aus einem Dropdown-Menü auswählen. Die Nutzer:innen haben den Eindruck, dass die Beantwortung dieser Frage ihnen (scheinbar) ermöglicht, die gewünschte Handlung durchzuführen, d. h. das Konto zu löschen. Sobald eine Antwort ausgewählt worden ist, erscheint ein Pop-up-Fenster, in dem den Nutzer:innen eine Lösung für das in ihrer Antwort genannte Problem angezeigt wird. Dieses Frage-Antwort-Verfahren hält die Nutzer:innen folglich beim Vorgang der Löschung ihres Kontos auf.

183. Zusätzlich dazu, dass die Löschung des Kontos besonders langwierig gestaltet wird, soll ein Mechanismus des Typs „*Schau, dort drüben*“ Nutzer:innen von der Löschung ihres Kontos ablenken, indem ihnen eine Lösung für ihren Beweggrund zum Verlassen der Social-Media-Plattform geboten wird. Dadurch wird die Ausübung des Rechts auf Löschung behindert und im weiteren Sinne werden die betroffenen Personen davon abgehalten, ihr Recht auszuüben.

Unbeständig – Dekontextualisierung (Anhang I Checkliste 4.5.2)

184. Und schließlich kann auch das irreführende Gestaltungsmuster der **Dekontextualisierung** zu finden sein, wenn Nutzer:innen ihr Konto löschen möchten.

Beispiel 60: Auf der Plattform XY ist der Link zur Deaktivierung oder Löschung des Kontos in der Registerkarte „Ihre XY-Daten“ zu finden.

185. Im Allgemeinen sollten die Begriffe, die für die Bezeichnung einer Datenschutzangelegenheiten gewidmeten Seite bzw. eines entsprechenden Abschnitts der Social-Media-Plattform verwendet werden, deutlich die Art der darin enthaltenen Informationen oder Kontrollfunktionen widerspiegeln. Es ist unwahrscheinlich, dass Durchschnittsnutzer Handlungen zur Löschung oder Deaktivierung ihres Kontos mit dem Verwalten ihrer Daten in Verbindung bringen. Im vorangegangenen Beispiel würden Nutzer:innen die Funktion zum Löschen ihres Kontos nicht auf einer Seite mit der Bezeichnung „Ihre XY-Informationen“ erwarten, die darauf anspielt, dass dort die eigenen Informationen angesehen und möglicherweise überarbeitet werden können. Stattdessen würden sie nach einer Seite „Allgemeines“ oder „Mein Konto löschen“ suchen. Aus Sicht der Nutzer:innen werden die Optionen so in einem aus dem Kontext gerissenen Umfeld platziert, was nicht den Erwartungen der Nutzer:innen entspricht.

Beispiel 61: Der Tab für die Löschung eines Kontos ist im Abschnitt „Eine Funktion Ihres Kontos löschen“ zu finden.

186. In diesem Beispiel könnten die Nutzer:innen den Titel des Abschnitts als bloßen Ort missverstehen, an dem einzelne Funktionen angepasst werden können. Nutzer:innen würden daher nicht erwarten, dass sich dort die Option zum Löschen des gesamten Kontos befindet. Dies erschwert es den Nutzer:innen, den richtigen Link zum Löschen des gesamten Kontos zu finden.
187. Das in den beiden vorstehenden Beispielen veranschaulichte irreführende Gestaltungsmuster der **Dekontextualisierung** könnte als Verstoß gegen Artikel 12 Absatz 2 DS-GVO angesehen werden, da die Nutzer:innen Schwierigkeiten hätten, den richtigen Ort zur Ausübung ihres Rechts auf Löschung zu finden.

c. Best Practices

Einheitliche Formulierungen: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 29).

Begriffsbestimmungen bereitstellen: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 29).

Verwendung von Beispielen: Eine Begriffsbestimmung ist im Anwendungsfall 1 zu finden (S. 30).

Folgen erläutern: Eine Begriffsbestimmung ist im Anwendungsfall 2c zu finden (S. 42).

Geräteübergreifende Einheitlichkeit: Eine Begriffsbestimmung ist im Anwendungsfall 3a zu finden (S. 51).

Für den Europäischen Datenschutzausschuss

Die Vorsitzende

(Andrea Jelinek)

4 ANHANG I: VERZEICHNIS DER KATEGORIEN UND ARTEN IRREFÜHRENDER GESTALTUNGSMUSTER

Das folgende Verzeichnis bietet einen Überblick über die Kategorien und die Arten irreführender Gestaltungsmuster innerhalb der einzelnen Kategorien. Ferner werden die Bestimmungen der DS-GVO aufgeführt, die am stärksten von den einzelnen Arten irreführender Gestaltungsmuster betroffen sind. Die Leser sollten beachten, dass, wie bereits erwähnt, der in Artikel 5 Absatz 1 Buchstabe a DS-GVO verankerte Grundsatz der Verarbeitung nach Treu und Glauben ein Ausgangspunkt für die Bewertung des Vorliegens irreführender Gestaltungsmuster ist. Dieser Grundsatz hat eine übergreifende Funktion und alle irreführenden Gestaltungsmuster wären – unabhängig von der Einhaltung anderer Datenschutzgrundsätze – mit diesem Grundsatz nicht vereinbar.⁸¹

Für jedes Muster enthält das Verzeichnis außerdem die Nummern der Beispiele und der entsprechenden Anwendungsfälle, damit die Leser diese schnell finden können.

Es sei darauf hingewiesen, dass dieses Verzeichnis nicht abschließend ist und irreführende Gestaltungsmuster daher auch in Anwendungsfällen auftreten können, für die im Text der Leitlinien kein Beispiel enthalten ist.

4.1 Überfrachtung

Nutzer:innen werden mit Massen von Anfragen, Informationen, Optionen oder Möglichkeiten überhäuft, um sie davon abzuhalten, fortzufahren, und sie zu veranlassen, bestimmte Praktiken im Zusammenhang mit Daten beizubehalten oder zu akzeptieren.

4.1.1 Ständige Aufforderungen⁸²

Nutzer:innen werden dazu gedrängt, mehr personenbezogene Daten zur Verfügung zu stellen, als es für die Zwecke der Verarbeitung erforderlich ist, oder einer anderen Verwendung ihrer Daten zuzustimmen, indem sie wiederholt aufgefordert werden, Daten bereit zu stellen oder in einen neuen Verarbeitungszweck einzuwilligen. Solche wiederholten Aufforderungen können über ein oder mehrere Geräte erfolgen. Dies endet wahrscheinlich damit, dass Nutzer:innen nachgeben, weil sie dessen überdrüssig sind, bei jeder Nutzung der Plattform die Anfrage ablehnen zu müssen und in ihrer Nutzung gestört zu werden.

Betroffene Vorschriften der DS-GVO:

- *Zweckbindung: Artikel 5 Absatz 1 Buchstabe b;*
- *Freiwillig erteilte Einwilligung: Artikel 7 in Verbindung mit Artikel 4 Nummer 11;*
- *Einwilligung für den bestimmten Fall: Artikel 7 Absatz 2.*

Beispiele: Anwendungsfall 1, Beispiele 1 und 2; Anwendungsfall 3a Beispiel 34 (Abbildung).

⁸¹ Siehe Rn. 9 dieser Leitlinien.

⁸² Dieses Muster steht in engem Zusammenhang mit einem Muster, das in der wissenschaftlichen Literatur als „Nagging“ bezeichnet wird.

4.1.2 Datenschutz-Labyrinth

Wenn Nutzer:innen bestimmte Informationen erlangen, eine bestimmte Kontrollfunktion nutzen oder ein Betroffenenrecht ausüben möchten, ist es für sie besonders schwierig, dies zu finden, da sie durch eine zu große Zahl von Seiten navigieren müssen, um zu den einschlägigen Informationen oder Kontrollfunktionen zu gelangen. Ihnen steht keine umfassende und vollständige Übersicht zur Verfügung. Es besteht die Wahrscheinlichkeit, dass Nutzer:innen aufgeben oder die einschlägigen Informationen oder Kontrollfunktionen übersehen.

Betroffene Vorschriften der DS-GVO:

- *Grundsatz der Transparenz: Artikel 5 Absatz 1 Buchstabe a und transparente Informationen: Artikel 12 Absatz 1;*
- *Grundsatz der Verarbeitung nach Treu und Glauben: Artikel 5 Absatz 1 Buchstabe a;*
- *Leicht zugängliche Informationen: Artikel 12 Absatz 1;*
- *Leichter Zugang zu den Rechten: Artikel 12 Absatz 2;*
- *Einwilligung in informierter Weise: Artikel 7 in Verbindung mit Artikel 4 Nummer 11;*

Beispiele: Anwendungsfall 2a Beispiel 17; Anwendungsfall 3a Beispiel 33; Anwendungsfall 3b Beispiel 37; Anwendungsfall 4 Beispiele 47 (Abbildung) und 48 (Abbildung); Anwendungsfall 5 Beispiel 51.

4.1.3 Zu viele Optionen

Den Nutzer:innen werden (zu) viele Auswahlmöglichkeiten zur Verfügung gestellt. Die Zahl der Wahlmöglichkeiten führt dazu, dass Nutzer:innen nicht mehr fähig sind, eine Entscheidung zu treffen, oder dass sie bestimmte Einstellungen übersehen, insbesondere wenn keine Informationen verfügbar sind. Die Folge kann sein, dass sie ihre Datenschutzpräferenzen oder -rechte schließlich aufgeben oder übersehen.

Betroffene Vorschriften der DS-GVO:

- *Grundsätze der Transparenz und Verarbeitung nach Treu und Glauben: Artikel 5 Absatz 1 Buchstabe a;*
- *Transparente Informationen: Artikel 12 Absatz 1.*

Beispiel: Anwendungsfall 3b Beispiel 35.

4.2 Überspringen

Gestaltung der Benutzeroberfläche oder des Nutzererlebnisses in einer Weise, dass die Nutzer:innen alle oder einige Datenschutzaspekte vergessen oder nicht bedenken.

4.2.1 Trügerische Bequemlichkeit

Die dateninvasivsten Funktionen und Optionen sind standardmäßig aktiviert. Beruhend auf dem Voreinstellungseffekt werden Personen dazu gebracht, eine vorab ausgewählte Option beizubehalten, sodass es unwahrscheinlich ist, dass Nutzer:innen diese ändern, selbst wenn sie die Möglichkeit dazu erhalten.

Betroffene Vorschriften der DS-GVO:

- *Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen:* Artikel 25 Absatz 1;
- *Einwilligung:* Artikel 4 Nummer 11 und Artikel 6 (rechtswidrige Praxis, eine Verarbeitung auf der Grundlage einer standardmäßig voreingestellten Einwilligung zu aktivieren).

Beispiele: Anwendungsfall 1 Beispiel 9; Anwendungsfall 3b Beispiele 39 und 40 (Abbildung); Anwendungsfall 5 Beispiel 55.

4.2.2 „Schau, dort drüben“

Eine datenschutzbezogene Handlung oder Information wird in Konkurrenz zu einem anderen Element gesetzt, das mit dem Datenschutz zusammenhängen kann oder nicht. Wählen Nutzer:innen diese ablenkende Option, werden sie wahrscheinlich die andere vergessen, selbst wenn diese ihrer ursprünglichen Absicht entsprach.

Betroffene Vorschriften der DS-GVO:

- *Grundsätze der Transparenz und Verarbeitung nach Treu und Glauben:* Artikel 5 Absatz 1 Buchstabe a;
- *Transparente Informationen:* Artikel 12 Absatz 1;
- *Ausübung der Rechte:* Artikel 12 Absatz 2.

Beispiele: Anwendungsfall 2c Beispiel 25; Anwendungsfall 3a Beispiel 29; Anwendungsfall 5 Beispiele 56 und 58.

4.3 Aufwühlen

Wirkt sich mittels Ansprechen von Emotionen oder visueller „Anreize“ auf die Wahl aus, die Nutzer:innen treffen.

4.3.1 Emotionale Steuerung⁸³

Verwendung von Formulierungen oder visuellen Elementen (z. B. Stil, Farben, Bilder usw.) in einer Weise, dass Nutzer:innen Informationen entweder in einer sehr positiven Art und Weise vermittelt werden, sodass sich Nutzer:innen gut, sicher oder belohnt fühlen, oder aber in einer stark negativen Art und Weise, die dazu führt, dass sich die Nutzer:innen ängstlich, schuldig oder bestraft fühlen. Eine solche Beeinflussung des emotionalen Zustands von Nutzer:innen kann sie zu Handlungen veranlassen, die ihren Datenschutzinteressen zuwiderlaufen.

⁸³ Dieses Muster steht in engem Zusammenhang mit einer Art von Muster, das als „*Spielen mit Emotionen*“ bezeichnet wird und unter anderem in Berichten zwischenstaatlicher Organisationen wie der Europäischen Kommission, Generaldirektion Justiz und Verbraucher vorkommt; Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., et al., Behavioural study on unfair commercial practices in the digital environment: *dark patterns and manipulative personalisation: final report*; Amt für Veröffentlichungen der Europäischen Union, 2022, <https://data.europa.eu/doi/10.2838/859030> und OECD (2022), „Dark commercial patterns“, Documents de travail de l'OCDE sur l'économie numérique, n° 336, Éditions OCDE, Paris, <https://doi.org/10.1787/44f5e846-en>. Angenommen

Betroffene Vorschriften der DS-GVO:

- *Grundsätze der Transparenz und Verarbeitung nach Treu und Glauben:* Artikel 5 Absatz 1 Buchstabe a;
- *Transparente Informationen:* Artikel 12 Absatz 1;
- *Ausübung der Rechte:* Artikel 12 Absatz 2;
- *Einwilligung eines Kindes:* Artikel 8;
- *Einwilligung in informierter Weise:* Artikel 7 in Verbindung mit Artikel 4 Nummer 11;

Beispiele: Anwendungsfall 1 Beispiele 4, 5 und 6; Anwendungsfall 5 Beispiel 52.

4.3.2 Vor aller Augen verborgen

Verwendung von grafischen Elementen oder Techniken für Informationen und Kontrollfunktionen bezüglich des Datenschutzes, die Nutzer:innen einen „Anreiz“ hin zu weniger restriktiven und somit stärker invasiven Optionen geben.

Betroffene Vorschriften der DS-GVO:

- *Grundsatz der Verarbeitung nach Treu und Glauben:* Artikel 5 Absatz 1 Buchstabe a;
- *Freiwillig erteilte Einwilligung:* Artikel 7 in Verbindung mit Artikel 4 Nummer 11;
- *Klare Informationen:* Artikel 12 Absatz 1;
- *Ausübung der Rechte:* Artikel 12 Absatz 2;

Beispiele: Anwendungsfall 1 Beispiel 8, Anwendungsfall 3a Beispiel 34 (Abbildung); Anwendungsfall 3b Beispiel 40 (Abbildung); Anwendungsfall 4 Beispiel 48.

4.4 Behindern⁸⁴

Nutzer:innen werden daran gehindert oder es wird ihnen der Weg versperrt, sich zu informieren oder ihre Daten zu verwalten, indem die jeweilige Handlung erschwert oder unmöglich gemacht wird.

4.4.1 Sackgasse

Während die Nutzer:innen Informationen oder eine Kontrollfunktion suchen, finden sie diese letztlich nicht, da ein weiterführender Link entweder nicht funktioniert oder überhaupt nicht verfügbar ist. Die Nutzer:innen sind nicht in der Lage, die betreffende Aufgabe zu erfüllen.

Betroffene Vorschriften der DS-GVO:

- *Leicht zugängliche Informationen:* Artikel 12 Absatz 1;
- *Ausübung der Rechte:* Artikel 12 Absatz 2;
- *Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen:* Artikel 25 Absatz 1.

⁸⁴ Diese Kategorie steht in engem Zusammenhang mit der Strategie „*Obstruction*“, die in Gray Colin M., Kou Yubo, Battles Bryan, Hoggatt Joseph und Toombs Austin L. 2018 definiert und beschrieben wird: The Dark (Patterns) Side of UX Design. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (Montreal QC, Canada) (CHI '18). ACM, New York, NY, USA, Artikel 534, 14 Seiten. <https://doi.org/10.1145/3173574.3174108>.

Beispiele: Anwendungsfall 1 Beispiele 10 und 11; Anwendungsfall 2a Beispiel 18; Anwendungsfall 3a Beispiele 30 und 31; Anwendungsfall 4 Beispiel 43.

4.4.2 Länger als erforderlich

Wenn Nutzer:innen versuchen, eine datenschutzbezogene Kontrollfunktion zu aktivieren, verläuft das Nutzererlebnis so, dass die Nutzer:innen mehr Schritte unternehmen müssen, als für die Aktivierung dateninvasiver Optionen erforderlich ist. Dies wird sie voraussichtlich davon abhalten, eine solche Kontrollfunktion zu aktivieren.

Betroffene Vorschriften der DS-GVO:

- *Leicht zugängliche Informationen:* Artikel 12 Absatz 1;
- *Ausübung der Rechte:* Artikel 12 Absatz 2;
- *Widerspruchsrecht:* Artikel 21 Absatz 1;
- *Widerruf der Einwilligung:* Artikel 7 Absatz 3;
- *Datenschutz durch Technikgestaltung (und datenschutzfreundliche Voreinstellungen):* Artikel 25 Absatz 1.

Beispiele: Anwendungsfall 1 Beispiel 7; Anwendungsfall 3a Beispiel 32; Anwendungsfall 4 Beispiel 50; Anwendungsfall 5 Beispiele 57 (Abbildung) und 58.

4.4.3 Irreführende Handlungen

Eine Diskrepanz zwischen den Informationen und verfügbaren Handlungen Nutzer:innen bringt diese dazu, etwas zu tun, was sie nicht beabsichtigen. Die Differenz zwischen dem, was die Nutzer:innen erwarten, und dem, was sie bekommen, wird sie voraussichtlich davon abhalten, ihren Weg fortzusetzen.

Betroffene Vorschriften der DS-GVO:

- *Transparente Informationen:* Artikel 12 Absatz 1;
- *Verarbeitung nach Treu und Glauben:* Artikel 5 Absatz 1 Buchstabe a.
- *Einwilligung in informierter Weise:* Artikel 7 Absatz 2 in Verbindung mit Artikel 4 Nummer 11.

Beispiele: Anwendungsfall 1 Beispiel 3; Anwendungsfall 3a Beispiel 28.

4.5 Unbeständig

Die Gestaltung der Benutzeroberfläche ist instabil und uneinheitlich, was den Nutzer:innen erschwert, die Art der Verarbeitung festzustellen, eine ordnungsgemäße Wahl hinsichtlich ihrer Daten zu treffen und herauszufinden, wo sich die verschiedenen Kontrollfunktionen befinden.

4.5.1 Fehlende Hierarchie

Bei den Informationen über den Datenschutz fehlt eine Hierarchie, sodass Informationen mehrfach erscheinen und auf verschiedene Weise dargestellt werden. Nutzer:innen dürften

durch diese Wiederholung verwirrt werden und anschließend nicht in der Lage sein, zu verstehen, wie ihre Daten verarbeitet werden und wie sie Kontrolle über sie ausüben können.

Betroffene Vorschriften der DS-GVO:

- *Leicht zugängliche Informationen:* Artikel 12 Absatz 1;
- *Ausübung der Rechte:* Artikel 12 Absatz 2.

Beispiele: Anwendungsfall 2a Beispiele 13 und 14.

4.5.2 Dekontextualisierung

Eine Information oder Kontrollfunktion mit Bezug zum Datenschutz befindet sich auf einer aus dem Zusammenhang gerissenen Seite. Es ist unwahrscheinlich, dass Nutzer:innen die Information oder Kontrollfunktion finden, da sie nicht intuitiv auf dieser speziellen Seite nach ihr suchen würden.

Betroffene Vorschriften der DS-GVO:

- *Leicht zugängliche Informationen:* Artikel 12 Absatz 1;
- *Transparente Informationen:* Artikel 12 Absatz 1;
- *Ausübung der Rechte:* Artikel 12 Absatz 2.

Beispiele: Anwendungsfall 3b Beispiele 41 und 42; Anwendungsfall 5 Beispiele 59 und 60.

4.5.3 Uneinheitliche Benutzeroberfläche

Eine Benutzeroberfläche ist in verschiedenen Kontexten nicht einheitlich (z. B. zeigt ein Datenschutz-Menü auf Mobiltelefonen und Desktop-Computern nicht dieselben Elemente) oder stimmt nicht mit den Erwartungen der Nutzer:innen überein (z. B. eine Option, deren Ort mit dem einer anderen Option getauscht wurde). Diese Unterschiede können dazu führen, dass Nutzer:innen die gewünschte Kontrollfunktion oder Information nicht finden oder dass sie aus reiner Gewohnheit mit einem Element der Benutzeroberfläche interagieren, obwohl diese Interaktion zu einer Datenschutzentscheidung führt, die die Nutzer:innen nicht wünschen.

Betroffene Vorschriften der DS-GVO:

- *Leicht zugängliche Informationen:* Artikel 12 Absatz 1;
- *Ausübung der Rechte:* Artikel 12 Absatz 2.

Beispiele: Anwendungsfall 3b Beispiel 39; Anwendungsfall 4 Beispiel 50.

4.5.4 Sprachliche Diskontinuität

Datenschutzinformationen werden nicht in der/den Amtssprache(n) des Landes bereitgestellt, in dem die Nutzer:innen wohnen, während dies bei dem Dienst selbst der Fall ist. Beherrschen Nutzer:innen die Sprache nicht, in der die Datenschutzinformationen bereitgestellt werden,

können sie diese nicht problemlos lesen und wissen daher voraussichtlich nicht, wie die Daten verarbeitet werden.

Betroffene Vorschriften der DS-GVO:

- *Verarbeitung nach Treu und Glauben:* Artikel 5 Absatz 1 Buchstabe a;
- *Verständliche Informationen:* Artikel 12 Absatz 1, Artikel 13 und Artikel 14;
- *Verwendung einer klaren und einfachen Sprache für die Informationen:* Artikel 12 Absatz 1, Artikel 13 und Artikel 14.

Beispiele: Anwendungsfall 2a Beispiel 16; Anwendungsfall 3a, Beispiele 26 (Abbildung) und 27; Anwendungsfall 4 Beispiel 44.

4.6 Im Dunkeln gelassen

Die Schnittstelle ist so konzipiert, dass Informationen oder Kontrollfunktionen mit Bezug zum Datenschutz verborgen werden oder Nutzer:innen im Ungewissen gelassen werden, wie ihre Daten verarbeitet werden und welche Art von Kontrolle sie darüber haben könnten.

4.6.1 Widersprüchliche Informationen

Den Nutzer:innen werden Informationen übermittelt, die einander in gewisser Weise widersprechen. Dies führt wahrscheinlich dazu, dass Nutzer:innen unsicher sind, was sie tun sollten und was die Folgen ihrer Handlungen sind, sodass sie voraussichtlich nichts unternehmen und einfach die Standardeinstellungen beibehalten.

Betroffene Vorschriften der DS-GVO:

- *Verarbeitung nach Treu und Glauben:* Artikel 5 Absatz 1 Buchstabe a;
- *Transparente Informationen:* Artikel 12 Absatz 1;
- *Einwilligung in informierter Weise:* Artikel 7 Absatz 2 in Verbindung mit Artikel 4 Nummer 11.

Beispiele: Anwendungsfall 2a Beispiel 12; Anwendungsfall 2c Beispiel 20; Anwendungsfall 3b Beispiel 36.

4.6.2 Mehrdeutige Formulierungen oder Informationen

Verwendung von mehrdeutigen und vagen Begriffen bei der Information von Nutzer:innen. Sie werden wahrscheinlich im Ungewissen darüber gelassen, wie die Daten verarbeitet werden oder wie sie Kontrolle über ihre personenbezogenen Daten ausüben können.

Betroffene Vorschriften der DS-GVO:

- *Verarbeitung nach Treu und Glauben:* Artikel 5 Absatz 1 Buchstabe a;
- *Transparente Informationen:* Artikel 12 Absatz 1;
- *Verwendung einer klaren und einfachen Sprache für die Informationen:* Artikel 12 Absatz 1;
- *Einwilligung in informierter Weise:* Artikel 7 Absatz 2 in Verbindung mit Artikel 4 Nummer 11;

- *Unvollständige Informationen:* Artikel 13;
- *Besondere Bestimmungen je nach Anwendungsfall,* z. B. Artikel 34 für Anwendungsfall 2c.

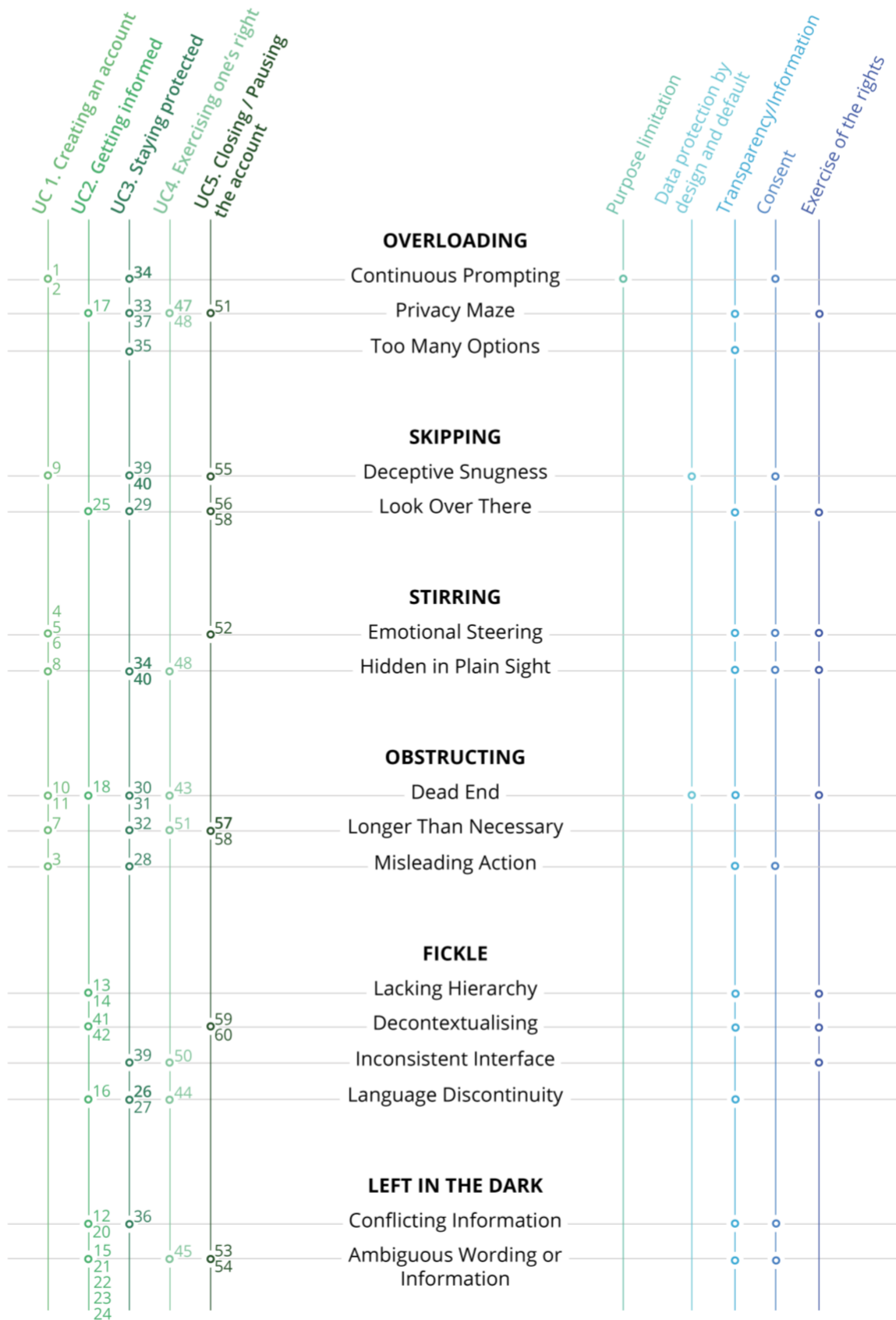
Beispiele: Anwendungsfall 2a Beispiel 15; Anwendungsfall 2c Beispiele 21, 22, 23 und 24; Anwendungsfall 4 Beispiel 45; Anwendungsfall 5 Beispiele 53 und 54.

LIFECYCLE

DECEPTIVE DESIGN OVERVIEW

GDPR PROVISIONS

All deceptive design go
against the fairness principle



5 ANHANG II: BEST PRACTICES

Die folgende Auflistung bietet einen Überblick über die in den Leitlinien am Ende der einzelnen Anwendungsfälle beschriebenen Best Practices. Diese können für die Gestaltung von Benutzeroberflächen verwendet werden, die die wirksame Umsetzung der DS-GVO erleichtern. Solche Best Practices können einen ersten Schritt auf dem Weg zu einer standardisierten Art und Weise bieten, wie Nutzer:innen ihre Daten wirksam kontrollieren und ihre Rechte wahrnehmen können.

Schnellzugriffe: Links zu Informationen, Handlungen oder Einstellungen, die Nutzer:innen bei der Verwaltung ihrer Daten und ihrer Datenschutzeinstellungen von praktischem Nutzen sein können, sollten überall dort verfügbar sein, wo die Nutzer:innen mit einer entsprechenden Information oder Erfahrung konfrontiert sind (z. B. *Links, die sie zu den einschlägigen Teilen der Datenschutzerklärung weiterleiten. Stellen Sie beispielsweise in der Datenschutzerklärung für jede Datenschutzzinformation einen Link bereit, der direkt zu den entsprechenden Datenschutzseiten auf der Social-Media-Plattform weiterleitet. Stellen Sie den Nutzer:innen einen Link zum Zurücksetzen des Passworts zur Verfügung. Werden Nutzer:innen beispielsweise über einen Aspekt der Verarbeitung informiert, werden sie gebeten, ihre diesbezüglichen Datenpräferenzen auf der entsprechenden Seite mit Einstellungen/Dashboard festzulegen. Stellen Sie im Nutzerkonto einen Link zur Löschung des Kontos bereit*).

Zusammengefasste Optionen: Zusammenfassung von Optionen, die denselben Verarbeitungszweck haben, sodass Nutzer:innen sie einfacher ändern können, dabei aber die Möglichkeit behalten, detailliertere Änderungen vorzunehmen. Wenn Social-Media-Plattformen zusammengefasste Optionen bieten, sollten diese keine unerwarteten oder nicht miteinander zusammenhängenden Elemente enthalten (z. B. Elemente mit unterschiedlichen Zwecken). Ist für die Verarbeitung eine Einwilligung erforderlich, müssen die zusammengefassten Optionen mit den EDSA-Leitlinien zur Einwilligung, insbesondere Rn. 42-44, im Einklang stehen. Nutzer:innen

Kontaktdaten: Die Kontaktadresse des Unternehmens für die Bearbeitung von Datenschutzanfragen sollte in der Datenschutzerklärung deutlich angegeben werden. Sie sollte in einem Abschnitt erscheinen, in dem die Nutzer:innen diese Angabe erwarten können, beispielsweise in einem Abschnitt über die Identität des Verantwortlichen, in einem rechtebezogenen Abschnitt oder in einem Abschnitt mit Kontaktdaten.

Erreichbarkeit der Aufsichtsbehörde: Angabe der genauen Bezeichnung der Aufsichtsbehörde und eines Links zu ihrer Website oder der dortigen speziellen Seite, auf der eine Beschwerde eingereicht werden kann. Diese Informationen sollten in einem Abschnitt erscheinen, in dem die Nutzer:innen sie erwarten können, beispielsweise in einem Abschnitt, der sich auf Rechte bezieht.

Überblick über die Datenschutzerklärung: Am Anfang/im Kopfteil der Datenschutzerklärung sollten Sie ein (ausblendbares) Inhaltsverzeichnis mit Überschriften und Unterüberschriften bereitstellen, aus dem die verschiedenen Passagen der Datenschutzhinweise ersichtlich sind. Die Namen der einzelnen Passagen führen die Nutzer:innen eindeutig zu den genauen Inhalten und ermöglichen es ihnen, den gesuchten Abschnitt schnell zu ermitteln und zu erreichen.

Änderungshistorien und Vergleich: Werden am Datenschutzhinweis Änderungen vorgenommen, machen Sie frühere Versionen mit dem Datum der Veröffentlichung zugänglich und heben Sie Änderungen hervor.

Einheitliche Formulierungen: Auf der Website werden für dieselben Datenschutzbestimmungen jeweils dieselben Formulierungen und Begriffsbestimmungen verwendet. Die in der Datenschutzerklärung verwendete Formulierung sollte derjenigen entsprechen, die auf der übrigen Plattform verwendet wird.

Begriffsbestimmungen bereitstellen: Werden ungewohnte oder fachspezifische Wörter oder Jargons verwendet, hilft die Bereitstellung einer Begriffsbestimmung in einfacher Sprache den Nutzer:innen beim Verständnis der Informationen, die ihnen zur Verfügung gestellt werden. Die Begriffsbestimmung kann direkt im Text erfolgen, wenn Nutzer:innen mit dem Mauszeiger über das betreffende Wort fahren, oder in einem Glossar zur Verfügung gestellt werden.

Hervorgehobene Datenschutzelemente: Elemente oder Handlungen mit Bezug zum Datenschutz werden auf einer Benutzeroberfläche, die dem betreffenden Thema nicht unmittelbar gewidmet ist, visuell auffällig dargestellt. Wenn beispielsweise auf der Plattform eine öffentliche Nachricht gepostet wird, sollten Steuerungsmöglichkeiten für die Verknüpfung des geografischen Standorts direkt verfügbar und deutlich sichtbar sein.

Einführung in den Datenschutz (Onboarding): Social-Media-Anbieter sollten im Rahmen des Anmeldeprozesses unmittelbar nach der Einrichtung eines Kontos Aspekte zum Datenschutz aufnehmen, damit die Nutzer:innen ihre Präferenzen problemlos entdecken und festlegen können. Dies kann beispielsweise dadurch geschehen, dass sie aufgefordert werden, ihre Datenschutzpräferenzen festzulegen, nachdem sie ihren ersten Freund hinzugefügt oder ihren ersten Post geteilt haben.

Verwendung von Beispielen: Neben obligatorischen Angaben, die den Zweck der Verarbeitung klar und präzise angeben, können Beispiele verwendet werden, um eine bestimmte Datenverarbeitung zu veranschaulichen, sodass sie für die Nutzer:innen konkreter und besser greifbar wird.

Angeheftete Navigationsleiste: Beim Lesen einer Seite zum Datenschutz kann das Inhaltsverzeichnis ständig auf dem Bildschirm angezeigt werden, sodass sich die Nutzer:innen stets auf der Seite verorten und dank Verlinkungen schnell im Inhalt navigieren können.

Zurück zum Seitenanfang: Fügen Sie am unteren Fuß der Seite oder als angeheftetes Element am unteren Ende des Fensters eine Schaltfläche für die Rückkehr zum Seitenanfang ein, um den Nutzer:innen die Navigation auf einer Seite zu erleichtern.

Benachrichtigungen: Benachrichtigungen können verwendet werden, um die Nutzer:innen für Aspekte, Änderungen oder Risiken im Zusammenhang mit der Verarbeitung personenbezogener Daten zu sensibilisieren (z. B. *wenn es zu einer Verletzung des Schutzes personenbezogener Daten kam*). Diese Benachrichtigungen können auf verschiedene Weise umgesetzt werden, beispielsweise durch Nachrichten im Posteingang, Pop-in-Fenster, feste Banner oben auf der Website usw.

Folgen erläutern: Wenn Nutzer:innen eine Datenschutzkontrollfunktion aktivieren oder deaktivieren oder ihre Einwilligung erteilen oder widerrufen wollen, informieren Sie sie auf neutrale Weise über die Folgen einer solchen Handlung.

Geräteübergreifende Einheitlichkeit: Ist die Social-Media-Plattform mittels verschiedener Geräte (z. B. Computer, Smartphone usw.) verfügbar, sollten sich die Einstellungen und Informationen bezüglich des Datenschutzes in den verschiedenen Versionen an denselben Orten befinden und über dieselben Pfade und Elemente in der Benutzeroberfläche (Menüs, Symbole usw.) zugänglich sein.

Datenschutzverzeichnis: Um eine einfache Orientierung durch die verschiedenen Abschnitte des Menüs zu ermöglichen, stellen Sie den Nutzer:innen eine leicht zugängliche Seite bereit, von der aus alle mit dem Datenschutz zusammenhängenden Handlungen und Informationen zugänglich sind. Diese Seite kann im Hauptnavigationsmenü des Anbieters, im Nutzerkonto, über die Datenschutzerklärung usw. zu finden sein.

Kontextbezogene Informationen: Zusätzlich zu einer umfassenden Datenschutzerklärung sollten zu dem für den Nutzer:innen am besten geeigneten Zeitpunkt kurze Informationen zur Verfügung gestellt werden, damit dieser spezifische, kontinuierliche Informationen über die Art und Weise erhält, wie seine Daten verarbeitet werden.

Selbsterklärende URL: Auf Seiten im Zusammenhang mit Datenschutzeinstellungen oder -informationen sollte eine Internetadresse verwendet werden, die deren Inhalt klar widerspiegelt. Beispielsweise könnte eine Seite, auf der die Kontrollfunktionen für den Datenschutz zentral zusammengefasst werden, eine URL wie [soziales-netzwerk.com]/datenschutzeinstellungen bereithalten.

Formular für die Ausübung der Rechte: Um den Nutzer:innen die Wahrnehmung ihrer Rechte aus der DS-GVO zu erleichtern, sollte ein spezielles Formular bereitgestellt werden, das die Nutzer:innen beim Verständnis ihre Rechte unterstützt und ihnen bei dieser Art von Anfragen Orientierungshilfe bietet.