

# DSGVO vs. Online-Dienste: Realität der Datenauskunft

*Daniela Pöhn*

## *Zusammenfassung*

Seit dem Inkrafttreten der europäischen Datenschutz-Grundverordnung stellt das Auskunftsrecht nach Art. 15 ein zentrales Instrument für Nutzertransparenz dar. Bisher publizierte Studien belegen jedoch eine Diskrepanz zwischen dem rechtlichen Anspruch und der praktischen Umsetzung durch Online-Dienste. Nachdem dies bei großen Online-Diensten durch verwandte Studien gezeigt wurde, analysiert dieser Artikel die Umsetzung bei (1) kleineren Diensten, die vorrangig in Deutschland agieren, und (2) Diensten, die mit sensiblen Daten nach Art. 9 oder anderen, sensiblen Daten arbeiten, basierend auf drei Studien. Es zeigt sich, dass auch hier eine Diskrepanz zwischen rechtlichem Anspruch und praktischer Umsetzung besteht, was insbesondere bei sensiblen Daten kritisch zu bewerten ist. Die Ergebnisse werden hinsichtlich der Implikationen für die Nutzenden und neuer Möglichkeiten durch die künstliche Intelligenz und die aktuellen politischen Entwicklungen diskutiert.

## *1. Einleitung*

Seit dem Inkrafttreten der europäischen Datenschutz-Grundverordnung (DSGVO) im Mai 2018 ist das Auskunftsrecht nach Art. 15 eines der neuen Rechte für Endnutzende, auch betroffene Personen genannt. Dieses Recht stärkt die Position der Nutzenden gegenüber Unternehmen und anderen Organisationen, die personenbezogene Daten verarbeiten. Es ermöglicht betroffenen Personen, Transparenz über die Speicherung und Verarbeitung ihrer personenbezogenen Daten bei Online-Diensten, sogenannten Controllern, zu verlangen. Darüber hinaus dient das Auskunftsrecht als Grundlage, um die Rechtmäßigkeit der Datenverarbeitung zu überprüfen und weitere Datenschutzrechte, wie etwa das Recht auf Berichtigung oder Löschung, geltend zu machen.

In der Literatur wurden bisher Anfragen nach Art. 15 DSGVO nur vereinzelt untersucht, beispielsweise wie Online-Dienste tatsächlich auf

Auskunftsanfragen, auch *Data Subject Access Requests* (DSARs) genannt, reagieren, welche Formate sie verwenden, wie verständlich ihre Antworten sind und wo sie scheitern. Diese Studien beschränken sich meist auf wenige große Online-Dienste (Pöhn/Gruschka 2025) oder bestimmte Aspekte, wie *Dark Patterns* (Löbel u. a. 2024) oder normierte Auskunftsmöglichkeiten (Leschke u. a. 2023). Pöhn u. a. (2023) zeigten, dass kleinere Online-Dienste häufig schlechter abschnitten, jedoch wurden nur wenige ausgewählte davon untersucht. Daher zeigt die Kurzzusammenfassung der Literatur, dass kleinere Dienste bisher kaum untersucht wurden. Von besonderem Interesse sind zudem Dienste, die mit sensiblen Daten arbeiten, die durch Art. 9 DSGVO besonders geschützt sind, da hier ein erhöhtes Maß an Transparenz und Kontrolle verlangt wird. Selbst wenn Nutzende ihre Daten freigeben, ist die Einhaltung der DSGVO elementar.

Daher werden hier (1) Online-Dienste, die sensible Daten speichern, und (2) kleinere, eher nationale oder regionale Online-Dienste analysiert. Dabei soll bspw. überprüft werden, ob wie bei Pöhn u. a. (2023) Online-Dienste aus Deutschland vorrangig per E-Mail-Anfragen annehmen und beantworten. Basierend auf den Analysen werden (3) die Ergebnisse bspw. hinsichtlich der Implikationen für die Nutzenden und neuer Möglichkeiten durch die künstliche Intelligenz diskutiert. Damit zeigt diese Veröffentlichung ein breiteres Bild bei der Umsetzung von Art. 15 DSGVO und diskutiert die Implikationen der gefundenen Ergebnisse.

Nachfolgend wird in Abschn. 2 der Stand der Forschung zusammengefasst, bevor in Abschn. 3 die grundlegende Methodik für die Erstellung der Online-Konten und die Untersuchung der Anfragen, Antworten und Daten beschrieben wird. In Abschn. 4 werden die Untersuchungen der Dienste, unterteilt in kleinere Dienste und Dienste mit sensiblen Daten, dargelegt und jeweils ein Zwischenfazit gezogen. Die Ergebnisse werden anschließend in Abschn. 5 diskutiert. Abschn. 6 schließt den Artikel mit einem Fazit und Ausblick.

## 2. Stand der Forschung

Während viele Veröffentlichungen zu Cookie-Bannern existieren, werden DSARs bisher verhältnismäßig selten betrachtet. Die meisten Veröffentlichungen betrachten die Nutzerperspektive, Dark Patterns, eine Methodik zur Veröffentlichung der Antworten und die DSARs bei ausgewählten Online-Diensten.

Petelka u. a. (2022) analysierten 38 DSARs von elf unterschiedlichen Organisationen durch Teilnehmer aus Indien, dem Vereinigten Königreich und den USA. Die Autoren betonen, dass die Teilnehmenden häufig Workarounds nutzen mussten, um an die eigenen Daten zu gelangen. Ebenfalls aus der Nutzerperspektive betrachteten Borem u. a. (2024) DSARs bei *Amazon*, *Facebook*, *Spotify* oder *Google*. Die Teilnehmenden zeigten sich enttäuscht, überrascht und verwirrt über die Antworten. Die Fragen der Teilnehmenden wurden selten durch die erhaltenen Daten beantwortet. Dies verdeutlicht ein Missverhältnis zwischen den Erwartungen der Nutzenden und der Realität von DSARs.

Pöhn u. a. (2023) untersuchten 27 Online-Dienste, wie *Google*, *Amazon* und *TikTok*, die überwiegend weltweit agieren. Zum Vergleich wurden weitere Online-Dienste gewählt, die sich auf den deutschsprachigen Raum beschränken. Die Autoren folgerten, dass Dienste, bei denen die Anfrage nach Art. 15 DSGVO einzig per E-Mail gestellt werden könne, diese manuell bearbeiten würden. Zudem zeigten die Autoren erste Dark Patterns auf, die sie während der Studie bemerkten. Ein Beispiel hierfür ist das Verstecken der Anfragefunktionalität. Basierend auf den Ergebnissen analysierten Löbel u. a. (2024) systematisch Dark Patterns bei 166 Online-Diensten. Bei 113 der untersuchten Online-Dienste konnten die Autoren insgesamt 238 Dark Patterns beobachten. Dabei entfielen 68 auf „*Obstructing*“ (drei Varianten), 42 auf „*Overloading*“ (drei Varianten), 34 auf „*Left in the Dark*“ (zwei Varianten), 37 auf „*Stirring*“ (zwei Varianten), 32 auf „*Fickle*“ (vier Varianten) und 25 auf „*Skipping*“ (drei Varianten). Damit verwendeten die Online-Dienste im Durchschnitt 1,43 Dark Patterns. Diese beobachteten Dark Patterns erschweren bis verhindern DSARs der Nutzenden.

Leschke u. a. (2024) stellten eine Methodik zur Veröffentlichung von DSGVO-Auskunftsantworten durch die Verwendung synthetischer Konten vor. Bei der exemplarischen Umsetzung zeigte sich, dass die Qualität der Auskünfte nicht zufriedenstellend im Sinne von vollständig und verständlich ist. Carrière u. a. (2025) veröffentlichten ihre Erfahrungen mit Datenspenden durch ihren verbesserten methodischen Ansatz, in dem Daten von realen Nutzern pseudonymisiert gespendet werden. Das Projekt TES-TER (Böning/Laufs 2024), welches sich mit der Transparenz und der nutzerfreundlichen Darstellung von Daten aus der Auskunft über die gespeicherten Daten beschäftigt, präsentierte erste Ideen für ein normiertes Auskunftsrecht. Ähnliche Ideen verfolgten auch Hansen u. a. (2023) und Leschke u. a. (2023).

Die genannten Erkenntnisse bei der Analyse der erhaltenen Daten wurden bei Einzelfallanalysen an den Beispielen von *X* (früher *Twitter*; Pöhn/Gruschka 2024) und *Facebook*, *Microsoft*, *Google*, *Apple*, *Amazon*, *LinkedIn* und *WhatsApp* (Pöhn/Gruschka 2025) bestätigt. Während Antworten zu Beginn des Inkrafttretens der DSGVO meist spärlich ausfielen, wurden diese mit wachsendem regulatorischem Druck umfangreicher, allerdings manchmal auf Kosten der Verständlichkeit. Zudem stellten einzelne Online-Dienste erst bei späteren Auskünften Daten bereit, die sie bereits früher erhoben und bei zwischenzeitlichen Auskünften nicht angegeben hatten. Besonders hervorgehoben wird dieses Verhalten am Beispiel von *Amazon* (Pöhn/Gruschka 2025). Damit zeigen sich große Online-Dienste nicht vollständig konform mit der DSGVO. Zugleich können mehrere Datensätze tiefere Einblicke in Geschäftspraktiken liefern, wie am Beispiel von *Uber* (Binns u. a. 2025) zu sehen. Die Autoren stellten basierend auf den Daten beispielsweise dynamische Preise und geringere Sicherheit fest, die Lebenskosten mit *Uber*-Fahrten decken zu können.

Dieser Überblick verdeutlicht, dass sich die bisherigen Studien hinsichtlich Art. 15 DSGVO vorwiegend auf bestimmte Aspekte, wie Dark Patterns und die Nutzendenperspektive, fokussierten oder wenige große Online-Dienste, wie Amazon, Google, Facebook und Apple, untersuchten. KMUs und andere Organisationen müssen jedoch ebenfalls die DSGVO umsetzen. Folglich fehlt eine breiter angelegte Analyse. Zugleich wurden bisher keine Dienste analysiert, die besonders sensible Daten (nach Art. 9) mit erhöhtem Schutzbedarf speichern.

### 3. Methodik

In diesem Abschnitt wird die grundlegende Methodik zum Erstellen eines Kontos, zur Abfrage der gespeicherten Daten und zur Analyse der so erhaltenen Daten basierend auf der Methodik von Leschke u. a. (2024) vorgestellt. Die einzelnen Schritte sind in Abb. 1 verdeutlicht und werden nachfolgend beschrieben.

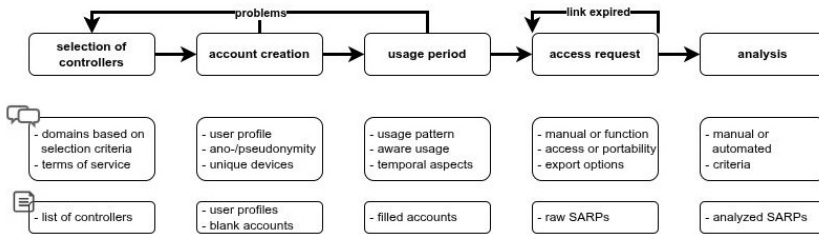


Abbildung 1: Die genutzte Methodik zur Analyse der Anfragen nach Art. 15 DSGVO (basierend auf Leschke u. a. 2024).

Die (1) Auswahl der Online-Dienste, auch *controllers* (Leschke u. a. 2024) genannt, erfolgt nach Regionalität, Größe bzw. der Kategorie der verarbeiteten sensiblen Daten. Um Interferenzen zu vermeiden, werden (2) neue Konten mit eigens dafür ausgewählten Endgeräten erstellt. Hierfür wird ein Nutzerprofil bzw. eine Persona passend zum Online-Dienst kreiert. Die (3) Nutzung erfolgt passend zum Ziel und, sofern möglich, ohne Einbeziehung Dritter. Beispielsweise wird für Sport-Apps ein Sportplan mit passendem Ziel entwickelt und die Nutzung der Chat-Funktion, die Unbeteiligte beeinträchtigen könnte, vermieden. Soweit die (4) DSARs über vorgefertigte Funktionen gestellt werden können, werden diese genutzt. Ansonsten wird eine vorgefertigte Blaupause für die Anfrage verwendet. Die Anfrage selbst wird genauso wie das Erhalten und Herunterladen der Daten nach dem Schema von Pöhn/Gruschka (2025) dokumentiert. Im Gegensatz zu Leschke u. a. (2024) ist das Ziel nicht die Veröffentlichung, sondern die (5) Analyse der Daten, die manuell erfolgt.

#### 4. Analysen

Nachfolgend werden die Ergebnisse der drei durchgeführten Studien vorgestellt. Die Studien wurden zwischen Oktober 2024 und August 2025 durchgeführt. Folglich stehen die analysierten Online-Dienste und Daten für den Zeitpunkt, an dem die jeweilige Studie durchgeführt wurde.

##### 4.1 DSARs von Diensten im deutschsprachigen Raum

Nachdem Pöhn u. a. (2023) neben weltweit agierenden auch wenige kleinere, auf deutschsprachige Nutzende ausgerichtete Online-Dienste unter-

suchten, deren Anfrageoptionen auf manuelle Bearbeitung der Anfragen hindeuten, sollten solche kleineren Online-Dienste im deutschsprachigen Raum genauer analysiert werden. Hierfür wurden 16 Online-Dienste (vgl. Tab. 1 im Anhang) ausgewählt, die entweder häufig genutzt werden oder Nischen bedienen. Die Studie wurde von März bis Mai 2025 durchgeführt.

Von diesen Online-Diensten haben vier (25 %; *Heise*, *MIFCOM*, *Kochbar* und *extraETF*) keine Antwort geliefert. Drei (18,75 %; *Hardwaredealz*, *NOZ* und *Merkur*) Online-Dienste meinten, aufgrund der fehlenden Speicherung von Daten – auch wenn ein Online-Konto erstellt wurde – keine Daten bereitstellen zu müssen. Von diesen Online-Diensten wurden zwei Benutzerkonten (12,5 %; *Hardwaredealz* und *NOZ*) nach der Anfrage ohne Erhalt von Daten gelöscht. Die verbliebenen neun (56,25 %) Online-Dienste antworteten vermutlich mit manuell zusammengestellten Daten, basierend auf Art der Anfrage und Zeit bis zur Antwort. Hierbei waren drei Antworten (18,75 %; *Nordbayern*, *Lecker* und *Süddeutsche*) entsprechend der Protokollierung der Eingaben unvollständig; zwei möglicherweise widersprüchlich in Hinblick auf die Datenschutzerklärung (12,5 %; *Finanztipp* und *Süddeutsche*); und eine (6,25 %; *Netzkino*) widersprüchlich in Hinblick auf die gesendeten Daten. Folglich sind während der Studie nur vier Antworten (25 %; *Gamestar*, *Moviepilot*, *Biallo* und *detektor.fm*) vollständig gewesen. Damit schnitt die Kategorie Unterhaltung am besten ab.

Die durchschnittliche Antwortzeit betrug 459 Stunden und 8 Minuten, also knapp über 19 Tage, was auf eine manuelle Bearbeitung hindeutet. Im gesamten Prozess wurden mehrere Dark Patterns nach Löbel u. a. (2024) und Pöhn u. a. (2023) identifiziert. Das Dark Pattern „*Longer than necessary*“ (Löbel u. a. 2024) beschreibt den verhältnismäßig langen Weg zur Anfrage, der beispielsweise bei *Süddeutsche* und *Merkur* protokolliert wurde. Teils wurden die Informationen auch ungeeignet dargestellt, was das Stellen der Anfrage zusätzlich erschwert. Dies wird auch „*Hidden in plain sight*“ (Löbel u. a. 2024) bzw. „*Hiding GDPR request information*“ und „*Hiding data from the user*“ (Pöhn u. a. 2023) genannt. „*Misleading action*“ (Löbel u. a. 2024) bezeichnet die Irreführung durch vage oder unklare Auswahlmöglichkeiten oder falsche Reiter, was beispielsweise bei *Lecker* dazu führte, den Reiter Datenschutzmanager ohne Erfolg zu durchsuchen. „*Conflicting information*“ (Löbel u. a. 2024) im Sinn von „*Left in the dark*“ (Löbel u. a. 2024) beschreibt widersprüchliche Darstellungen, welche beispielsweise beim Kopieren von E-Mail-Adressen verwirren, wenn sich die auf der Website angezeigte kopierbare E-Mail-Adresse und die verlinkte und damit durch den Nutzer dann kopierte und neu eingefügte

E-Mail-Adresse unterscheiden. Mehrfach wurde auch das Pattern „*Dead end*“ (Löbel u. a. 2024) identifiziert, wenn die Anfrage an einer Stelle ein plötzliches Ende fand. Ferner wurden mehr Angaben (bspw. eine zusätzliche postalische Adresse) bei der Anfrage als „*Continuous prompting*“ (Löbel u. a. 2024) bzw. „*Requiring too much/no proof of identification*“ (Pöhn u. a. 2023) gewertet. Insgesamt nutzte jeder der untersuchten Online-Dienste mindestens ein Dark Pattern oder eine andere erkennbare strukturelle Barriere. Damit wurden mehr Dark Patterns als bei Löbel u. a. (2024) gefunden, die insbesondere größere Online-Dienste analysierten. Bei der Art der Dark Patterns zeigt sich, dass größere Dienste häufig überladen sind, während es bei kleineren eher grundlegend an Zugänglichkeit und Transparenz mangelt.

Die Ergebnisse werfen Fragen zur praktischen Wirksamkeit des Auskunftsrechts auf und verdeutlichen strukturelle Schwächen bei der Durchsetzung der Betroffenenrechte. Betroffene müssen mit Hürden bei der Wahrnehmung ihrer Rechte rechnen. Zugleich fehlt die Transparenz, ob und in welchem Umfang personenbezogene Daten von Online-Diensten verarbeitet werden, nachdem die meisten Dienste nur unvollständige Auskünfte geben.

#### 4.2 DSARs von Diensten mit sensiblen Daten in vier Ländern

Der Schutz personenbezogener Daten gewinnt im digitalen Zeitalter insbesondere bei Online-Diensten, die sensible Daten wie allgemein Gesundheits- und im Speziellen Menstruationsdaten verarbeiten, zunehmend an Bedeutung. Dies wird auch durch Art. 9 DSGVO deutlich. Um einen ersten Überblick über den Umgang mit diesen Daten in unterschiedlichen Ländern zu erhalten, wurden landesspezifische Datenschutzgesetze aus der EU, Großbritannien, Kalifornien sowie Australien verglichen und analysiert, wie ausgewählte Online-Dienste diese Regelungen umsetzen. Hierfür wurden die Datenschutzerklärungen der Online-Dienste *Clue* (DE), *My Possible Self* (UK), *MyFitnessPal* (US) und *FatSecret* (AUS) (vgl. Tab. 2 im Anhang) untersucht und bewertet. In der praktischen Studie wurden virtuelle Maschinen eingerichtet, um die Nutzer-Standorte Deutschland, Großbritannien, Kalifornien und Australien zu simulieren und anschließend die vier Online-Dienste zu nutzen, was zu 16 Testfällen führte. Nach Anfrage und Erhalt der Daten wurden Kriterien wie die Zugänglichkeit der Anfrage

und die Datenqualität und -minimierung untersucht. Diese Studie wurde im Zeitraum von Oktober bis Dezember 2024 durchgeführt.

Zunächst wird in diesem Abschnitt auf die DSARs und die dadurch erhaltenen Daten eingegangen. Die Ergebnisse der Analyse der Datenschutzerklärungen werden im Zwischenfazit aufgegriffen.

Die App *Clue* (DE) ermöglichte eine einfache Anfrage in allen Ländern. Die Antwortzeiten variierten zwischen den Ländern von 14 (Deutschland) bis 21 (Australien) Tagen. Daten wurden im JSON-Format bereitgestellt, was für Nutzende ohne technische Kenntnisse nicht einfach verständlich ist. Die erhaltenen Daten stimmen soweit mit den Datenschutzerklärungen überein, jedoch werden laut eigenen Angaben in Deutschland mehr Nutzungsdaten (bspw. Google-Anzeigen-ID und Anzahl der Anzeigen-IDs) für die technische Verbesserung der App verwendet.

Im Vergleich zu den anderen bei dieser Studie untersuchten Online-Diensten, gestaltete sich der Anfrageprozess bei *MyFitnessPal* (US) am kompliziertesten. Nach einer ersten Antwort folgt mit zeitlichem Abstand die finale Bereitstellung der Daten. Bevor die gespeicherten Daten heruntergeladen werden konnten, musste sich der Antragsteller per E-Mail und Verifikationscode authentisieren. Die Daten selbst werden in einer passwortgeschützten Excel-Datei bereitgestellt. Die Analyse der Daten zeigt erhebliche Unterschiede in Umfang und Qualität zwischen den untersuchten Ländern: 3.323 Zeilen (Deutschland), 166 Zeilen (Großbritannien), 475 Zeilen (USA) und 753 Zeilen (Australien) bei vorher festgelegter Nutzung und identischen Datenschutzeinstellungen. Bei einem Blick in die Datensätze konnten mehrere Leerzeilen in den Datensätzen für die Länder USA und Australien entdeckt werden. Der deutlichste Unterschied ist beim Datensatz für die deutsche Nutzung feststellbar: Lediglich 358 der 3.323 Zeilen beziehen sich auf das eigene Benutzerkonto. Die übrigen Zeilen enthalten personenbezogene Daten zweier anderer, realer Nutzender<sup>1</sup>, inklusive Gewicht, Körpergröße und BMI. Bei der weiteren Analyse fällt auf, dass nicht alle Daten bei den Benutzerkonten für Großbritannien, die USA und Australien korrekt und vollständig sind. Für viele eingegebene Werte wird beispielsweise NULL zurückgeliefert.

Die Anfrage bei *My Possible Self* (UK) muss per E-Mail gestellt werden, wobei die zunächst gefundene E-Mail-Adresse zu einer Fehlermeldung führte. Die an eine weitere E-Mail-Adresse gestellten Anfragen wurden

---

1 Wir haben im Nachgang an die Studie die Datenschutzbeauftragten informiert, jedoch keine Rückmeldungen erhalten.

in keinem der Fälle beantwortet. Ein ähnliches Ergebnis liefert *FatSecret* (AUS), welches keine der Anfragen beantwortet.

Das Ergebnis der Datenanfragen liefert differenzierte Ergebnisse. Lediglich ein Online-Dienst (*Clue* aus DE) antwortete auf alle vier DSARs innerhalb der gesetzlichen Frist und stellte die Daten bereit. Zwei der vier Online-Dienste (UK, AUS) antworteten nicht. Die Form, in der die Daten bereitgestellt wurden, unterschied sich je nach Dienst. Ein Dienst (*MyFitnessPal* aus US) übermittelte zudem Daten von weiteren Nutzenden, was ein meldepflichtiger Datenschutzvorfall ist. Nachdem die Daten sich je nach Land unterschieden, weist dies auf eine manuelle Bearbeitung hin. Das Ergebnis kann folglich bei weiteren Studien möglicherweise nicht reproduziert werden.

#### 4.3 DSARs von Diensten in mehreren Kategorien mit sensiblen Daten

Um eine größere Anzahl an unterschiedlichen Diensten mit sensiblen Daten nach Art. 9 DSGVO oder anderen, eher sensiblen Daten zu analysieren, wurden mehrere Online-Dienste in den Kategorien Menstruationsapps, Fitness- und Gesundheitsapps, Schlaf-Tracking-Apps, Apps zu Religion und Spiritualität, LGBTQ+-Selbsthilfe-Apps und Dating-Apps (vgl. Tab. 3 im Anhang) ausgewählt. Für die Nutzung wurden eine weibliche und eine männliche Persona erstellt sowie passende Aktivitäten bzw. Angaben vorab überlegt. So stellt die Nutzung der Menstruationsapps einen simulierten Zyklus dar. Anschließend wurden die Daten angefordert. Nachdem viele Online-Dienste nicht oder nicht ausreichend antworteten, wurde auf die Auswertung der Daten verzichtet. Diese Studie wurde im Zeitraum von März bis August 2025 durchgeführt.

Bei Menstruations-Apps antworteten mehrere Anbieter (*MyCalendar*, *LadyCycle* und *Uvuvue*), dass keinerlei personenbezogene Daten zentral gespeichert würden. Ein Export der lokal gespeicherten Daten war nicht in jedem Fall möglich. Zwei weitere Anbieter (*Flo* und *Clue*) versendeten eine passwortgeschützte ZIP-Datei, wobei die Schritte zur Anfrage nicht selbstklärend (elf Teilschritte) bzw. die Bereitstellung der Daten in manchen Aspekten nicht datenschutzfreundlich (Nutzung eines weiteren Dienstes) erscheinen.

Dating-Apps sperrten vermehrt das Konto, teils bereits bei der Anmeldung (*Bumble* und *Plenty of Fish*) und teils nach Anfrage der Daten nach Art. 15 DSGVO (*Hinge* und *OkCupid*). *Hinge* gestaltete den Prozess der

Anfrage und Verifikation selbst transparent, auch wenn keine Daten geschickt und das Konto gesperrt wurden. *Tinder* stellte als Ausnahme die angeforderten Daten nach mehreren, zeitlich versetzten Verifikationsschritten bereit.

Zwei der getesteten Schlaf-Tracking-Apps (*Sleep* und *Sleep Monitor*) speichern laut Aussage der Anbieter personenbezogene Daten nur lokal. Eine Antwort (*Calm*) blieb aus, während zwei Apps (*Sleep Cycle* und *Samsung Health*) eine Möglichkeit zum Export der Daten bereitstellten.

Bei den Apps zu Religion und Spiritualität konnte eine Anfrage (*Evermore*) nicht zeitnah beantwortet werden, da die für den Datenschutz zuständige Person im Urlaub war. Ein weiterer Anbieter (*Abide*) verstand die Anfrage zunächst als Wunsch auf Löschung. Die anschließend geschickten Screenshots genügten ebenfalls nicht den Anforderungen. Ähnlich unzureichend war die Antwort des Anbieters einer weiteren App (*Glauben leben*), für den es unklar war, welche Daten im Rahmen der Anfrage gemeint waren. Bei zwei Apps (*Bible* und *Cogito*) konnten Datenanfragen gestellt und schließlich Daten zur Verfügung gestellt werden.

Bei LGBTQ+-Selbsthilfe-Apps blieben in den allermeisten Fällen (*PrideMantra*, *Kalda* und *Lex*) die Anfragen unbeantwortet. Während eine Anfrage über einen integrierten Support-Button bei *Voda* unbeantwortet blieb, wurde eine E-Mail zeitnah beantwortet und die Daten konnten heruntergeladen werden. Bei *Taimi* sollte für die Anfrage zur Authentifizierung zusätzlich ein Selfie in einer bestimmten Pose gemacht werden, auch wenn bei der Anmeldung kein Bild erforderlich war. Nach Äußerung der Bedenken hierbei wurden die angeforderten personenbezogenen Daten nach 24 Stunden bereitgestellt.

Fitness- und Gesundheits-Apps bieten ein gemischtes Bild. Mehrere Anbieter (*Feeletics*, *Jefit*, *Seven – 7 Minute Workout* und *Google Fit*) entsprachen der Anfrage ohne Probleme. Bei anderen war wiederum die Mithilfe des Supports notwendig (bspw. *Nike Training Club*), was jedoch nicht immer (*Adidas Running* und *Strava*) zum Erfolg führte. Mehrere Anbieter (*8fit* und *MyFitnessPal*) löschten nach Anfrage das Konto, während ein weiterer Online-Dienst (*FitOn*) nie antwortete.

Die Ergebnisse zeigen, dass Online-Dienste, die mit sensiblen Daten nach Art. 9 DSGVO oder anderen, eher sensiblen Daten arbeiten, nicht zwangsläufig DSGVO-konform agieren. Besonders kritisch ist die Sperrung oder Löschung mehrerer Konten nach Anfragen nach Art. 15 DSGVO zu betrachten. Dies betrifft auch *MyFitnessPal*, welcher in der Studie, beschrieben in Abschn. 4.2, bereits negativ durch die Zusendung von Daten Dritter

auffiel. Folglich konnte zwar das in der vorherigen Studie erzielte Ergebnis (Daten Dritter in erhaltenen Daten enthalten) nicht verifiziert werden, jedoch ist das neue Ergebnis nicht konformer mit der DSGVO. *Clue* wiederholte das gute Bild, auch wenn kleinere Aspekte verbessert werden könnten. Die laut mehreren Online-Diensten rein lokale Speicherung konnte im Rahmen der Studie nicht verifiziert werden und soll folglich zukünftig betrachtet werden.

## 5. Diskussion

In diesem Abschnitt werden die im vorangegangenen Abschnitt erzielten Ergebnisse unter Einbezug der Literatur diskutiert.

### 5.1 Diskussion der Studien und Ergebnisse

Zusammenfassend offenbaren die Studien eine Diskrepanz zwischen gesetzlichen Anforderungen und der praktischen Umsetzung des Auskunftsrechts bei Online-Diensten. Viele der analysierten Umsetzungen scheitern an der technischen Reife, der Ausgestaltung oder der Transparenz. Zugleich zeigen sich Unterschiede zwischen den Online-Diensten. Insbesondere eher kleinere, nationale Online-Dienste setzen auf Anfragen per E-Mail und mit entsprechend manueller, zeitaufwändiger Bearbeitung, die nicht unbedingt konform zur DSGVO sind. Aber auch Online-Dienste, die sensible Daten nach Art. 9 DSGVO oder andere, eher sensible Daten speichern, schneiden überraschend schlecht ab. Die beschriebenen Studien zeigen, dass nicht zwingend der rechtliche Rahmen das Problem ist, sondern die Art und Weise, wie Unternehmen ihn interpretieren und umsetzen. Ohne klare technische Standards und Frameworks, verbraucherfreundliche Gestaltung mit Blick auf den Nutzenden und zugleich Betroffenen und behördliche Kontrollen mit entsprechenden Konsequenzen bleibt das Auskunftsrecht ein Versprechen. Genau diese Hilfestellungen und Konsequenzen scheinen bei verhältnismäßig kleinen Diensten besonders wichtig zu sein. Folgestudien könnten ein breiteres Bild der DSAR-Realität zeigen und somit in Kombination mit Wissenschaftskommunikation auf bestehende Probleme aufmerksam machen.

Wenn Nutzende ihr Recht auf Information über verarbeitete persönliche Daten faktisch kaum wahrnehmen oder verstehen können, besteht die Ge-

fahr eines strukturellen Ungleichgewichts zugunsten datenverarbeitender Unternehmen. Insbesondere vulnerable Gruppen, bspw. ältere Menschen, Menschen mit Behinderung, Menschen mit geringerer digitaler Bildung oder finanziell schlechter gestellte Menschen, laufen Gefahr, systematisch ausgeschlossen zu werden, da ihnen der Zugang zu den Funktionen zur Durchsetzung ihrer Rechte, die sie vielleicht nicht einmal kennen, verwehrt bleibt. Entsprechend der digitalen Teilhabe sollte deshalb der Zugang für Nutzende zu den eigenen Daten vereinfacht werden.

Auch wenn stellenweise die Nutzung von Personas bei Online-Diensten gegen die Nutzungsrichtlinien verstößt und daher die Löschung von Konten bei der Nutzung möglich ist, können nationale Gesetze diese Regelungen außer Kraft setzen (Leschke u. a. 2024). Laut mehreren psychologischen Verbänden, wie dem Berufsverband Deutscher Psychologinnen und Psychologen und der Deutschen Gesellschaft für Psychologie, ist Täuschung nur dann akzeptabel, wenn beispielsweise ausschließlich dadurch ein wissenschaftlicher Mehrwert geschaffen werden kann und keine Alternative ohne Täuschung existiert. Bei den vorgestellten Studien konnten durch die Nutzung von Personas und dedizierten Geräten bzw. virtuellen Maschinen Interferenzen und Nachteile vermieden werden, die bspw. auftreten würden, wenn reale Konten verwendet würden. Bei Betrachtung der durchgeführten Studien wird zudem deutlich, dass noch mehr Online-Dienste und Kategorien, bspw. Apps für Kinder, betrachtet werden müssen, um einen umfassenden Überblick zu erhalten.

## 5.2 Chancen und Risiken von Sprachmodellen

Insbesondere in den Abschn. 4.1 und 4.2 wurden unvollständige oder falsche Datensätze bereits angesprochen. Dies deckt sich mit den Erkenntnissen anderer Studien (Pöhn/Gruschka 2024; 2025). Zugleich wurden bei diesen Studien teils Probleme bei der Datenminimierung festgestellt. Wenn große Sprachmodelle oder Empfehlungssysteme auf historischen, aber unvollständigen, intransparenten oder inkorrekten Daten beruhen, kann dies zu falschen Ergebnissen führen.

Außerdem können zu viele Daten ein umfassendes Profil eines gläsernen Menschen generieren, was wiederum für passende Produktplatzierungen oder auch Empfehlungen für Krankenkassen genutzt werden kann. Dies bezieht sich nicht nur auf die bei den Online-Diensten gespeicherten Daten, sondern auch auf die durch Werbe-Tracking und Datenhandel gesam-

melten Daten (Dachwitz/Meineck 2025). Durch die bereits existierenden Daten können Bewegungsprofile abgelesen werden, was sich zumindest teilweise auch durch die erhaltenen Daten bei DSARs nachvollziehen lässt (Pöhn/Gruschka 2024; 2025). Entsprechend der neuen Entwicklungen im Bereich der künstlichen Intelligenz und Sprachmodelle und der damit vereinfachten Auswertungsmöglichkeiten von großen Datenmengen ist die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten von großer Bedeutung.

Zugleich können Sprachmodelle und erklärbare künstliche Intelligenz womöglich zukünftig helfen, die Daten den Nutzenden besser zu erklären und greifbarer zu machen. Die Erklärbarkeit war nicht der Fokus der hier vorgestellten Studien, jedoch waren viele Daten eher maschinenlesbar als verständlich. Zusätzliche Erklärungen, wie sie durch manche große Online-Dienste realisiert werden, konnten nicht gefunden werden. Die Nutzung von Sprachmodellen und erklärbarer künstlicher Intelligenz für die Erklärbarkeit und Verständlichkeit der angefragten Daten erfordert allerdings weitere Forschung, zumal neue Gefahren möglich sind, beispielsweise wenn Nutzende unreflektiert sensible Daten in Systeme einspeisen, die niedrige Datenschutzstandards aufweisen.

### 5.3 Schaden durch die Nutzung der Daten

Nachdem bei den Online-Diensten mit sensiblen personenbezogenen Daten kaum Transparenz besteht, kann der Nutzende nicht absehen, welcher Schaden potenziell angerichtet werden kann. Bedingt durch das Privacy Paradox (Gerber u. a. 2018) bzw. das Problem, dass Dienste im Internet bereits viele Daten haben und dadurch ein vorsichtigerer Umgang für weniger relevant gehalten wird als bspw. eine bequeme Nutzung (Teuschel u. a. 2023), können mehr Daten gespeichert und potenziell genutzt werden als noch vor wenigen Jahrzehnten. In Hinblick auf die Überwachung durch Tracking (Dachwitz/Meineck 2025) kann der potenzielle Schaden beispielsweise bei Menstruationsapps (Souto/Müller 2025) durch geänderte politische Situationen weitreichende Folgen haben. Letztlich könnten die so erhobenen und gesammelten Daten für Regierungen und Behörden genutzt werden, sofern eine solche Nutzung rechtlich erlaubt ist. Durch die globale Welt können Daten von deutschen Nutzerinnen in den USA gespeichert werden, was je nach politischer Lage Fragen aufwerfen kann.

Dies zeigt zugleich das Missbrauchspotential und wie schnell die Sicherheit der Nutzerinnen in Gefahr sein kann (Malki u. a. 2024).

## 6. Fazit

In diesem Artikel wurden DSARs für Dienste im deutschsprachigen Raum und Dienste mit sensiblen Daten gestellt und die Daten analysiert. Im deutschsprachigen Raum antworteten viele Online-Dienste nicht oder nicht korrekt auf die Anfragen. Die erhaltenen Daten waren häufig nicht vollständig. Um Dienste mit sensiblen Daten zu analysieren, wurden zwei Studien durchgeführt. Es zeigte sich, dass Online-Dienste mit sensiblen Daten diese besser schützen könnten. Auch bei der breiter angelegten Studie mit Online-Diensten aus mehreren Kategorien wurde deutlich, dass Verbesserungsbedarf bei Anfragen und beim Herunterladen der Daten besteht. Zudem wurden mehrere Konten nach dem Stellen der Anfrage entweder deaktiviert oder gelöscht. Die Studien verdeutlichen somit die Diskrepanz zwischen dem rechtlichen Anspruch auf Transparenz und den tatsächlichen Praktiken der Online-Dienste hinsichtlich des Auskunftsrechts. Die bestehenden, in Studien dokumentierten Praktiken im Umgang mit personenbezogenen Daten führen zu einem potenziellen Missbrauch der gesammelten Informationen. Zugleich verschärfen mangelnde Sensibilität und Kenntnis von bestehenden Rechten die Problematik. Folglich sind weitere Arbeiten notwendig, um eine möglichst einfache Teilhabe – im Kontext von Art. 15 DSGVO von der Anfrage bis zur Betrachtung der eigenen Daten – zu ermöglichen.

## Literatur

- Binns, Reuben; Stein, Jake; Datta, Siddhartha; Van Kleek, Max und Shadbolt, Nigel (2025): Not Even Nice Work If You Can Get It; A Longitudinal Study of Uber's Algorithmic Pay and Pricing. In: *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency (FAcT '25)*. New York: Association for Computing Machinery (ACM), S. 1484–1497. <https://doi.org/10.1145/3715275.3732099>
- Böning, Fabiola und Laufs, Uwe (2024): Betroffenenrechte in der digitalen Selbstvermessung. In: Michael Friedewald, Alexander Roßnagel, Christian L. Geminn, Murat Karaboga und Stephan Schindler (Hrsg.): *Data Sharing – Datenkapitalismus by Default? Privatheit und Selbstbestimmung in der digitalen Welt*. Baden-Baden: Nomos, S. 301–323 <https://doi.org/10.5771/9783748940173>

- Borem, Arthur; Pan, Ellen; Obielodan, Olufunmilola; Roubinowitz, Aurelia und Dovichi, Luca (2024): Data Subjects' Reactions to Exercising Their Right of Access. In: *33rd USENIX Security Symposium, Philadelphia, PA, USA, August 14–16, 2024*. <https://www.usenix.org/system/files/usenixsecurity24-borem.pdf>
- Carrière, Thijs C.; Boeschoten, Laura; Struminskaya, Bella; Janssen, Heleen L.; de Schipper, Niek C. und Araujo, Theo (2025): Best practices for studies using digital data donation. *Quality & Quantity - International Journal of Methodology*, 59 (Suppl 1), S. 389–412. <https://doi.org/10.1007/s11135-024-01983-x>
- Dachwitz, Ingo und Meineck, Sebastian (04. November 2025): Databroker Files - Das Wichtigste zur Spionage-Gefahr durch Handy-Standortdaten in der EU. <https://netzpolitik.org/2025/databroker-files-das-wichtigste-zur-spionage-gefahr-durch-handy-standortdaten-in-der-eu/> (besucht am 23.01.2026).
- Gerber, Nina; Gerber, Paul und Volkamer, Melanie (2018): Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, 77, S. 226–261. <https://doi.org/10.1016/j.cose.2018.04.002>
- Hansen, Malte; Gruschka, Nils und Jensen, Meiko (2023): Introducing the Concept of Data Subject Rights as a Service Under the GDPR. In: Steffen Schiffner, Sébastien Ziegler und Meiko Jensen (Hrsg.): *Privacy Symposium 2023. Data Protection Law International Convergence and Compliance with Innovative Technologies (DPLICIT)*. Cham: Springer, S. 17–31. [https://doi.org/10.1007/978-3-031-44939-0\\_2](https://doi.org/10.1007/978-3-031-44939-0_2)
- Leschke, Nicola; Kirsten, Florian; Pallas, Frank und Grünewald, Elias (2023): Streamlining Personal Data Access Requests: From Obstructive Procedures to Automated Web Workflows. In: Irene Garrigós, Juan Manuel Murillo Rodríguez und Manuel Wimmer (Hrsg.): *Web Engineering. ICWE 2023. Lecture Notes in Computer Science*, Band 13893. Cham: Springer, S. 111–125. [https://doi.org/10.1007/978-3-031-34444-2\\_9](https://doi.org/10.1007/978-3-031-34444-2_9)
- Leschke, Nicola; Pöhn, Daniela und Pallas, Frank (2024): How to Drill into Silos: Creating a Free-to-Use Dataset of Data Subject Access Packages. In: Meiko Jensen, Cédric Lauradoux und Kai Rannenberg (Hrsg.): *Privacy Technologies and Policy, 12th Annual Privacy Forum, APF 2024, Karlstad, Sweden, September 04–05, 2024. Proceedings*. Cham: Springer, S. 132–155. [https://doi.org/10.1007/978-3-031-68024-3\\_7](https://doi.org/10.1007/978-3-031-68024-3_7)
- Löbel, Alexander; Schäfer, René; Püschel, Hanna; Güney, Esra und Meyer, Ulrike (2024): Access Your Data... if You Can: An Analysis of Dark Patterns Against the Right of Access on Popular Websites. In: Meiko Jensen, Cédric Lauradoux und Kai Rannenberg (Hrsg.): *Privacy Technologies and Policy, 12th Annual Privacy Forum, APF 2024, Karlstad, Sweden, September 04–05, 2024. Proceedings*. Cham: Springer, S. 23–47. [https://doi.org/10.1007/978-3-031-68024-3\\_2](https://doi.org/10.1007/978-3-031-68024-3_2)
- Malki, Lisa Mekioussa; Kaleva, Ina; Patel, Dilisha; Warner, Mark und Abu-Salma, Ruba (2024): Exploring Privacy Practices of Female mHealth Apps in a Post-Roe World. In: *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems (CHI '24)*. New York: Association for Computing Machinery (ACM), Artikel 576, S. 1–24. <https://doi.org/10.1145/3613904.3642521>

- Petelka, Justin; Oreglia, Elisa; Finn, Megan und Srinivasan, Janaki (2022): Generating Practices: Investigations into the Double Embedding of GDPR and Data Access Policies. In: *Proceedings of the ACM Human-Computer Interaction*. Band 6, Ausgabe CSCW2. New York: Association for Computing Machinery (ACM), Artikel 518, S. 1–26. <https://doi.org/10.1145/3555631>
- Pöhn, Daniela; Mörsdorf, Niklas und Hommel, Wolfgang (2023): Needle in the Haystack: Analyzing the Right of Access According to GDPR Article 15 Five Years after the Implementation. In: *Proceedings of the 18th International Conference on Availability, Reliability and Security, ARES '23*. New York: Association for Computing Machinery (ACM), Artikel 91, S. 1–10. <https://doi.org/10.1145/3600160.3605064>
- Pöhn, Daniela und Gruschka, Nils (2024): Past and Present: A Case Study of Twitter's Responses to GDPR Data Requests. In: Kai Rannenbergh, Prokopios Drogkaris und Cédric Lauradoux (Hrsg.): *Privacy Technologies and Policy, 11th Annual Privacy Forum, APF 2023, Lyon, France, June 01–02, 2023. Proceedings*. Cham: Springer Nature Switzerland, S. 57–84. [https://doi.org/10.1007/978-3-031-61089-9\\_4](https://doi.org/10.1007/978-3-031-61089-9_4)
- Pöhn, Daniela und Gruschka, Nils (2025): Qualitative In-Depth Analysis of GDPR Data Subject Access Requests and Responses from Major Online Services. In: *Proceedings of the 11th International Conference on Information Systems Security and Privacy - Volume 1*. ICISSP. Setúbal: INSTICC, SciTePress, S. 149–156. <https://doi.org/10.5220/00130930000003899>
- Souto, Luana Mathias und Müller, Jörg (2025): Legal and Ethical Challenges of Femtech: Protecting Women's Data & Rights in the Age of Surveillance Capitalism. In: *Companion Proceedings of the ACM on Web Conference 2025 (WWW '25)*. New York: Association for Computing Machinery (ACM), S. 2796–2798. <https://doi.org/10.1145/3701716.3716881>
- Teuschel, Moritz; Pöhn, Daniela; Grabatin, Michael; Dietz, Felix; Hommel, Wolfgang und Alt, Florian (2023): 'Don't Annoy Me With Privacy Decisions!' — Designing Privacy-Preserving User Interfaces for SSI Wallets on Smartphones. *IEEE Access*, Ausgabe 11, S. 131814–131835. <https://doi.org/10.1109/ACCESS.2023.3334908>

## Anhang

Tab. 1: Ausgewählte Dienste im deutschsprachigen Raum.

| Kategorie    | Online-Dienst-Name                                              |
|--------------|-----------------------------------------------------------------|
| Finanzen     | Finanztip, extraETF, Biallo                                     |
| Nachrichten  | Nordbayern, Neue Osnabrücker Zeitung (NOZ), Süddeutsche, Merkur |
| Computer     | Heise, Hardwaredealz, MIFCOM                                    |
| Rezepte      | Kochbar, Lecker                                                 |
| Unterhaltung | Netzkino, Moviepilot, Gamestar, detektor.fm                     |

Tab. 2: Ausgewählte Dienste mit sensiblen Daten.

| App-Name         | Herkunftsland | Kategorie                             |
|------------------|---------------|---------------------------------------|
| Clue             | Deutschland   | Menstruations-App                     |
| My Possible Self | UK            | Psychische Gesundheits-App            |
| MyFitnessPal     | USA           | Tracking-App f. Ernährung und Fitness |
| FatSecret        | Australien    | Abnehm-App                            |

Tab. 3: Ausgewählte Dienste in mehreren Kategorien mit sensiblen Daten.

| Kategorie                          | App-Name                                                                                                                 |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Menstruations-App                  | Flo, Clue, Lady Cycle, Uvuvview, Periodenkalender                                                                        |
| Dating-Apps                        | Tinder, Bumble, Hinge, OkCupid, Plenty of Fish                                                                           |
| Schlaf-Tracking-Apps               | Sleep as Android, Sleepcycle, Sleep Monitor, Calm, Samsung Health                                                        |
| Apps zu Religion und Spiritualität | Glauben.leben, Abide, Cogito, Bible App, Evermore                                                                        |
| LGBTQ+-Selbsthilfe-Apps            | Voda, Pride Mantra, Kalda, Lex, Taimi                                                                                    |
| Fitness- und Gesundheits-Apps      | Nike Training Club, Freeletics, Jefit, Seven, 8Fit, GoogleFit, Strava, MyFitnessPal, FitOn, Adidas Training by Runtastic |

