DSRI Herbstakademie 2025

Bernzen / Heinze / Steinrötter

2025
ISBN 978-3-406-84186-6
C.H.BECK

arbeitung ihrer Daten und machen von ihren Betroffenenrechten nach der DSGVO Gebrauch. So thematisieren Datenschutzaufsichtsbehörden in ihren Tätigkeitsberichten zuletzt Eingaben im Zusammenhang mit Identitätsverifikationen – insbesondere im Kontext von Retourenprozessen, Online-Gaming-Plattformen und E-Payment-Diensten.[28]

Zentrale Aspekte aus Nutzersicht sind:

- Transparenz über Art und Umfang der Datenverarbeitung;
- Nachvollziehbarkeit des Verifikationsprozesses;
- Kontrolle über die eigenen Daten;
- Vertrauen in die Sicherheit der Datenverarbeitung;
- Minimierung der preiszugebenden personenbezogenen Daten.

4.2 Best Practices

Im Hinblick auf die Transparenz können Kunden vor der Verifikation über den genauen Zweck etwa wie folgt informiert werden: „Zur Prävention von Betrug und Missbrauch bitten wir Sie, Ihre Identität zu verifizieren, bevor wir Ihre Rückerstattungsanfrage bearbeiten." Der Ablauf des Verifikationsprozesses sollte Schritt für Schritt erläutert werden, einschließlich der Information, welche Daten verarbeitet werden. Es muss klar kommuniziert werden, sollte ein spezialisierter Dienstleister die eigentliche Verifikation durchführen und welche Daten diesem zugänglich gemacht werden.

Es bietet sich an, Kunden darüber zu informieren, dass die Identitätsverifikation freiwillig ist und welche alternativen Möglichkeiten zur Verfügung stehen. Beispiel: „Sollten Sie keine Identitätsverifikation durchführen wollen, können Sie alternativ [spezifische Alternativen nennen, z. B. Rücksendung des Produkts] wählen." Um die Akzeptanz weiter zu stärken, könnten Plattformen ihren Nutzern vermehrt Wahlmöglichkeiten bieten – etwa durch abgestufte Verifikationsverfahren gemäß Art. 8 eIDAS-Verordnung („Low Assurance" vs. „High Assurance") oder durch Privacy Dashboards, wie sie von der ENISA und dem Europäischen Datenschutzausschuss empfohlen werden.[29]

Es sollte betont werden, dass die Ablehnung der Verifikation keine negativen Auswirkungen auf die zukünftige Nutzung des Dienstes hat. Entscheidend ist, dass die Ablehnung der Identitätsverifikation nicht zu einer unverhältnismäßigen Benachteiligung führen darf – etwa zum Verlust des Rückerstattungsanspruchs. Dies ergibt sich nicht nur aus dem Grundsatz der Freiwilligkeit (Art. 7 DSGVO), sondern auch aus dem Transparenzgebot (Art. 5 Abs. 1 lit. a DSGVO).

Die Speicherdauer der Ausweisdaten (typischerweise 5 Tage) muss klar kommuniziert werden.

Zudem wäre es denkbar, durch Anreizmechanismen wie Rabatte oder bevorzugten Versand bei vollständiger Verifikation einen positiven Anreiz zu schaffen, wie es auch wirtschaftliche Studien vorschlagen.[30]

---

[28] Vgl. Tätigkeitsbericht der Berliner Beauftragten für Datenschutz und Informationsfreiheit 2023, S. 93 ff.

[29] Vgl. ENISA, *Privacy Enhancing Technologies and Privacy by Design*, S. 12 ff.

[30] Vgl. Price Waterhouse Coopers, *The Future of Digital Identity in Customer Onboarding*, S. 18 ff.

5 Unternehmensperspektive

5.1 Herausforderungen

Unternehmen, die Onlineplattformen betreiben, sehen sich bei der Identitätsverifikation mit einem komplexen Anforderungsprofil konfrontiert. Sie müssen einen Balanceakt zwischen verschiedenen, teilweise konkurrierenden Zielen bewältigen: Einerseits gilt es, regulatorische Vorgaben einzuhalten und Betrugsrisiken effektiv zu minimieren. Andererseits muss der Verifikationsprozess nutzerfreundlich und wirtschaftlich gestaltet werden, um Kunden nicht durch übermäßige Hürden zu verlieren. Die Integration von Identitätsverifikationslösungen stellt Unternehmen vor mehrere Herausforderungen:

- Implementierung rechtlich konformer Verifikationsprozesse unter Berücksichtigung von DSGVO, GwG und weiteren regulatorischen Anforderungen;
- Gewährleistung einer positiven User Experience trotz notwendiger Sicherheitsmaßnahmen;
- Kosteneffizienz bei gleichzeitiger Erfüllung hoher Sicherheitsstandards;
- Management von Drittanbieterbeziehungen bei ausgelagerter Verifikation.

5.2 Best Practices

Zur Minimierung von Datenschutzrisiken entwickeln Unternehmen verschiedene Strategien:

- Implementierung technischer und organisatorischer Schutzmaßnahmen;
- Regelmäßige Überprüfung und Aktualisierung der Verifikationsprozesse;
- Schulung von Mitarbeitern im Umgang mit sensiblen Kundendaten;
- Entwicklung von Notfallplänen für potenzielle Datenschutzvorfälle.

Einige Unternehmen gehen inzwischen über klassische Maßnahmen hinaus und nutzen KI-gestützte Verhaltensanalysen, um ungewöhnliche Muster frühzeitig zu erkennen – etwa durch Machine-Learning-Modelle, die betrugsanfällige Transaktionen in Echtzeit identifizieren. Zudem setzen Pioniere auf Self-Sovereign Identity (SSI-)Modelle,[31] bei denen Nutzer ihre Identitätsdaten dezentral selbst verwalten und nur selektiv freigeben – was sowohl Sicherheit als auch Datenschutz stärkt. Diese Ansätze erfordern allerdings ein Umdenken in der Systemarchitektur sowie die Bereitschaft zur Zusammenarbeit mit neuen Technologiepartnern.[32]

Die technische Implementierung der Identitätsverifikation muss sowohl höchste Sicherheitsstandards als auch datenschutzrechtliche Anforderungen erfüllen. In der Praxis bedeutet dies:

- Beschränkung auf wesentliche Identifikationsmerkmale;
- Löschung der Ausweiskopien nach erfolgreicher Verifikation (typischerweise nach 5 Tagen);
- Keine dauerhafte Speicherung vollständiger Ausweisdaten;
- Speicherung ausschließlich auf Servern innerhalb der EU (typischerweise in Deutschland);

---

[31] Vgl. *Degen/Emmert,* Degen/Emmert, § 6 Elektronische Identitäten und Vertrauensdienste, Rn. 49.

[32] Vgl. European Banking Authority, *Guidelines on ICT and security risk management,* Rn. 53 ff.; KPMG, *Digital Identity Verification: Trends and Risks,* S. 9 ff.

- Automatisierte Dokumentenprüfung;
- Verschlüsselte Übertragung über TLS;
- Verschlüsselte Speicherung der Daten während der Verarbeitungszeit;
- Strikte Zugriffskontrollen und -protokollierung;

Der technische Prozess kann so gestaltet werden, dass er maximale Sicherheit bei minimaler Datenspeicherung gewährleistet:

- Der Kunde lädt das Ausweisdokument über ein gesichertes Portal hoch;
- Die automatisierte Prüfung erfolgt unmittelbar;
- An das anfragende Unternehmen wird nur das Ergebnis (bestanden/nicht bestanden) übermittelt;
- Die Ausweisdaten selbst werden nicht dauerhaft gespeichert;
- Eine Verknüpfung der Ausweisdaten mit dem Kundenprofil findet nicht statt;

Wichtig ist dabei die Beschränkung auf eine reine Echtheitsprüfung. Ein Abgleich mit behördlichen Registern oder eine weitergehende Identitätsfeststellung findet nicht statt.

6 Fazit & Ausblick

Im beschriebenen Fallbeispiel kann eine risikobasierte Identitätsverifikation dazu beitragen, Missbrauch frühzeitig zu erkennen. Wäre dem Kunden bekannt gewesen, dass bei mehrfachen hochpreisigen Reklamationen eine Verifikation erfolgt, hätte dies möglicherweise abschreckende Wirkung entfaltet. Alternativ hätte der Händler – durch die Kombination aus historischer Verhaltensanalyse und adaptiver Identitätsverifikation – den Vorgang als risikobehaftet einstufen und gezielt eine zusätzliche Prüfung anstoßen können.

Dieses Szenario verdeutlicht, dass Identitätsverifikation nicht als pauschales Kontrollinstrument eingesetzt werden sollte, sondern als situativ aktivierbares Tool im Rahmen eines datenschutzkonformen Risikomanagements. So kann Betrug effektiv begegnet werden, ohne legitime Kunden zu belasten.

Die digitale Identitätsverifikation ist in einer zunehmend vernetzten Welt kein optionales, sondern ein unverzichtbares Instrument zur Gewährleistung von Sicherheit, zur Betrugsprävention und zur Aufrechterhaltung des Vertrauens auf Onlineplattformen. Die zukünftige Entwicklung der Identitätsverifikation wird maßgeblich von technologischen Innovationen und europäischen Initiativen geprägt sein. In den nächsten 5 bis 10 Jahren ist mit folgenden Trends zu rechnen:

- KI-gestützte Verhaltensanalysen und adaptive Systeme: Die Rolle von Künstlicher Intelligenz wird weiter zunehmen.[33] KI-Modelle werden immer präziser in der Lage sein, betrugsanfällige Muster in Echtzeit zu erkennen und dynamische Anpassungen der Verifikationsstufe vorzunehmen. Dies ermöglicht eine noch feinere Granularität bei der Risikobewertung und schont die Kundenerfahrung der überwiegenden Mehrheit ehrlicher Nutzer.
- Verbindliche Etablierung des EU Digital Identity Wallet: Eine zentrale Rolle werden europäische Initiativen spielen, allen voran das geplante EU Digital Identity Wallet. Dieses digitale Identitätsbündel wird voraussichtlich eine sichere und vertrauenswürdige Möglichkeit bieten, sich online zu identifizieren und Daten auszutauschen. Unternehmen, die dieses Wallet integrieren, können von einer höheren Akzeptanz und standardisierten, interoperablen Verifikationsverfahren profitieren. Dies könnte die Not-

[33] Vgl. *Maaß,* Borges/Keil, § 2 Geschäftsmodelle, Rn. 46.

wendigkeit proprietärer Identitätslösungen reduzieren und die Compliance im europäischen Binnenmarkt erleichtern. Das Wallet zielt darauf ab, die verschiedenen Vertrauensniveaus der eIDAS-Verordnung (niedrig, substanziell, hoch) einheitlich abzubilden.[34]

- Fokus auf Datenminimierung und Privacy-by-Design: Der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) wird weiterhin eine zentrale Leitlinie bleiben. Zukünftige Verifikationslösungen werden darauf ausgelegt sein müssen, so wenig personenbezogene Daten wie möglich zu verarbeiten, während gleichzeitig die Wirksamkeit gegen Betrug gewährleistet bleibt. Konzepte wie Privacy Dashboards[35] werden an Bedeutung gewinnen, um Nutzern mehr Kontrolle und Transparenz über ihre Daten zu ermöglichen.
- Interoperabilität und Standardisierung: Eine größere Interoperabilität zwischen verschiedenen Identitätsverifikationssystemen und eine stärkere Standardisierung der technischen und rechtlichen Rahmenbedingungen sind wünschenswert. Dies würde die Komplexität für Unternehmen reduzieren und die Nutzerfreundlichkeit über Plattformgrenzen hinweg verbessern.

Die Herausforderung für Gesetzgeber und Unternehmen wird darin bestehen, einen Rahmen zu schaffen, der Innovation fördert, ohne die Grundrechte der Nutzer zu gefährden. Der Spagat zwischen effektiver Betrugsprävention und dem Schutz der informationellen Selbstbestimmung bleibt die zentrale Aufgabe, die es auch in Zukunft zu meistern gilt.

Literatur

Beimowski, Joachim/Gawron, Sylwester: Beck'sche Kompakt-Kommentare Passgesetz Personalausweisgesetz, München 2018.

Berlit, Wolfgang/Meyer, Claus/Kröner, Lars: Hamburger Kommentar Gesamtes Medienrecht, 4. Aufl., Baden-Baden 2021.

Borges, Georg/Hilber, Marc: Beck-Online-Kommentar IT-Recht, 18. Edition, München 2025.

Borges, Georg/Keil, Ulrich: Big Data Rechtshandbuch, Nomos-Kommentar, 1. Aufl., Baden-Baden 2024.

Britz, Thomas/Indenhuck, Moritz: The Rise of the Online-You: Auf dem Weg zu digitalen Identitäten, RDi 2023.

Buchner, Benedikt/Kühling, Jürgen: Datenschutzgrundverordnung BDSG Kommentar, 4. Aufl., München 2024.

Degen, Thomas/Emmert, Ulrich: Elektronischer Rechtsverkehr, 3. Aufl., München 2025.

Ehmann, Eugen/Selmayr, Martin: Beck'sche Kurz-Kommentare, DS-GVO Kommentar, 3. Aufl., München 2024.

Gabel, Detlev/Taeger, Jürgen: DSGVO-BDSG-TTDSG Kommentar, 4. Aufl., Frankfurt am Main 2022.

Gola, Peter/Heckmann, Dirk: Datenschutzgrundverordnung, Bundesdatenschutzgesetz, Kommentar, 3. Aufl., München 2022.

Herberger, Maximilian/Sorge, Christoph/Wächter, Michael/Weth, Stephan: Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl., München 2019.

Holznagel, Bernd/Hoeren, Thomas/Sieber, Ulrich: Handbuch Multimedia-Recht, 62. Ergänzungslieferung, München Juni 2024.

Hornung, Gerrit/Simitis, Spiros, Spiecker genannt Döhmann, Indra: Datenschutzrecht, Nomos-Kommentar, 2. Aufl., Baden-Baden 2024.

Katko, Peter: Checklisten zur Datenschutz-Grundverordnung (DSGVO), 2. Aufl., München 202.

Mimberg, Jörg/Omlor, Sebastian/Schäfer, Frank: Zahlungsdiensteaufsichtsgesetz Kommentar, 1. Aufl., München 2022

Paal, Boris/Pauly, Daniel: Beck'sche Kompakt-Kommentare Datenschutzgrundverordnung, 3. Aufl., München 2021.

[34] Vgl. *Britz/Indenhuck,* RDi 2023, 289, Rn. 40.

[35] Vgl. *Herberger/Sorge,* Weth/Herberger/Wächter/Sorge, XIV. Datenschutz durch IT, Rn. 4.

Ruge, Kay: Praxis der Kommunalverwaltung, 1. Fassung, München 2018.

Scaraggi-Kreitmeyer, Annamaria: Geldwäschebekämpfung für Steuerberater, 1. Aufl., München 2023.

Schantz, Peter/Wolff, Heinrich Amadeus: Das neue Datenschutzrecht, Datenschutzgrundverordnung und Bundesdatenschutzgesetz in der Praxis, 1. Aufl., München 2017.

Hinweis: KI kam für Recherche und Zusammenfassungen zum Einsatz. Die Ausgaben der KI wurden eigenständig geprüft und überarbeitet.

Verkettung von Profilen als Risiko bei der Auftragsverarbeitung

Tilmann Fleck/Johannes Nehlsen
Julius-Maximilians-Universität
gustav.fleck@uni-wuerzburg.de; johannes.nehlsen@uni-wuerzburg.de

Zusammenfassung

Die Nutzung insbesondere von Clouddiensten wirft gerade dann datenschutzrechtliche Fragen auf, wenn Auftragsverarbeiter auch eigene Dienste betreiben oder Daten aus der Auftragsverarbeitung eigenständig weiterverarbeiten. Dieser Beitrag beleuchtet die Risiken solcher Profilverkettungen und zeigt auf, wie Verantwortliche und Auftragsverarbeiter diesen Herausforderungen rechtlich, technisch und organisatorisch begegnen können.

Der Beitrag arbeitet das Risiko heraus, dass Auftragsverarbeiter personenbezogene Daten nicht nur im Auftrag, sondern daraus auch für eigene Zwecke nutzen können – etwa durch Profiling oder Dienstverknüpfungen. Dabei verschwimmen die Rollen zwischen Verantwortlichem und Auftragsverarbeiter. Ferner werden die rechtlichen Grundlagen (DSGVO, ePrivacy-Richtlinie, Data Act) analysiert, Praxisbeispiele (z. B. Microsoft, AWS) aufgezeigt und Lösungsansätze aus der Praxis wie vertragliche Zusicherungen, technische Schutzmaßnahmen und gesetzliche Regelungen erörtert. Fazit: Echte Auftragsverarbeitung ohne Eigeninteresse ist selten – Transparenz und Kontrolle sind entscheidend.

1 Rechtliche Einordung

Viele Clouddienste lösen bei Datenschutzbeauftragten und Aufsichten große Skepsis aus. Als Elefant im Raum der wirklichen Rechtsprobleme dieser Clouddienste, der nur selten entdeckt wird, ist folgendes Dilemma: Ein Auftragsverarbeiter ist oft nicht nur Auftragsverarbeiter, vielmehr werden die im Zusammenhang mit der Auftragsverarbeitung stehenden Daten selbst auch verarbeitet. Darüber hinaus werden auch weitere Dienste – ohne ihrerseits Auftragsverarbeiter zu sein – teilweise auch direkt an die Nutzer angeboten. Wie kann man sich als Verantwortlicher oder Auftragsverarbeiter diesem Risiko, der verschwimmenden Rollen von Verantwortlichem oder der möglichen Verkettung zwischen diesen Diensten stellen?[1]

1.1 Rolle des Verantwortlichen und des Auftragsverarbeiters

In der DSGVO ist grundsätzlich die Verantwortung beim Verantwortlichen. Im Rahmen der Auftragsverarbeitung liegen spezielle Pflichten bei Auftragsverarbeiter. Diese klare Rollentrennung findet schon im Bereich der Telekommunikation seine Grenzen, da ein Leistungsgestand, etwa Microsoft Teams als eine Kommunikationslösung aus dem

[1] Ob in sollen Fällen dagegen auch eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO vorliegt, ist nicht Gegenstand dieses Beitrages.

Lizenzpaket Microsoft 365 in Teilen der Regulierung durch die nationale Umsetzung der RL 2002/58/EG fällt (Kommunikationsvorgang an sich) und in Speicherung unter eine Auftragsverarbeitung nach Art. 28 DSGVO.

1.2 Rechtsgrundlage für die Offenlegung durch den Verantwortlichen

Nach der Definition der Art. 4 Nr. 2 DSGVO stellt auch eine Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung eine Form der Datenverarbeitung dar. Insoweit ist zu prüfen, ob für den Verantwortlichen die Offenlegung durch eine Zweckänderung nach Art. 6 Abs. 4 DSGVO denkbar ist[2] oder regelmäßig berechtigte Drittinteressen auf für den sendenden Verantwortlichen nach Art. 6 Abs. 1 lit. f DSGVO vorliegen.[3] Schwieriger kann sich dies bei Behörden gestalten, wenn die betroffenen Daten im Rahmen der gesetzlichen Aufgabenerfüllung verarbeitet werden.[4] Gleichwohl bieten etwa § 25 Abs. 2 BDSG oder Art. 5 Abs. 2 BayDSG entsprechende Öffnungen für Datenübermittlungen an.

1.3 Weiternutzung von Daten als Auftragsverarbeiter

Der Beitrag geht hier über das enge Verständnis von Profiling im Sinne des Art. 4 Nr. 4 DSGVO hinaus. Eine Verkettung im Sinne dieses Beitrages umfasst auch das Risiko, dass der Auftragsverarbeiter personenbezogene Daten unter der strengen Zweckbindung der Auftragsverarbeitung für sich selbst als eigener Verantwortlicher nutzt oder durch weitere eigene Dienste des Anbieters diese Daten aus der Nutzung mit Nutzungsdaten (in personenbezogener Form) aus der Auftragsverarbeitung verketten könnte.

Wenn der Auftragsverarbeiter die Daten weiternutzt, kommt es zu einer sogenannten eigenverantwortlichen Datenverarbeitung durch den Auftragsverarbeiter. Diese eigenverantwortliche Datenverarbeitung ist trotz ihrer mangelnden expliziten gesetzlichen Grundlage ein in der Praxis häufig aufzufindendes Konstrukt:

Problematisch ist in diesem Zusammenhang der in Art. 5 Abs. 1 lit. b DSGVO normierte Grundsatz der Zweckbindung. Dagegen gestattet Art. 6 Abs. 4 DSGVO jedoch gerade eine Verarbeitung der Daten zu anderen als den bei Erhebung vorgelegenen Zwecken, sodass vielmehr ein Weg von dem Grundsatz der Zweckbindung hin zu einer Interessenabwägung erkennbar ist.[5]

Die französische Datenschutzaufsicht „Commission Nationale de l'Informatique et des Libertés (CNIL)" hat zu Beginn des Jahres 2022 zur Möglichkeit der eigenverantwortlichen Datenverarbeitung Stellung genommen.[6] In dieser Stellungnahme kommt die CNIL zu dem Schluss, dass eine Verarbeitung durch den Auftragsverarbeiter auch durch eigene Zwecke möglich ist. Bei Vorliegen einer einschlägigen Rechtsgrundlage ist nach Art. 28 Abs. 3 S. 1, Art. 6 Abs. 4 DSGVO eine eigenverantwortliche Datenverarbeitung

---

[2] Skeptisch bereits *Giakoumopoulos/Buttarelli/O Flaherty,* Handbuch zum europäischen Datenschutzrecht, S. 148 f.

[3] Siehe etwa *Buchner/Petri,* in: Kühling/Buchner DSGVO, Art. 6 Rn. 146a f.

[4] Europäischer Datenschutzausschuss, Guidelines 1/2024 on processing of personal data based on Article 6(1)(f), GDPR, Version 1.0, Rn. 98 f.

[5] *Eichenhofer,* ePrivacy, S. 369; *ders.,* PinG 2017, 135 (140).

[6] Zur Pressemitteilung der CNIL vom 11.1.2022: https://www.cnil.fr/fr/sous-traitants-la-reutilisation-de-donnees-confiees-par-un-responsable-de-traitement; *Neumann/Fasshauer/Montagne/Chausse,* La CNIL précise les conditions de réutilisation des données par les sous-traitants, abrufbar unter: https://www.lexology.com/library/detail.aspx?g=1f99058c-b4a4-4568-8a19-e2c0571757ab, einzig bezugnehmend darauf in der Literatur *Strassemeyer,* DSB 2022, 56 (56 ff.).