Über die fehlgeleitete Kommunikation von Risiken im Datenschutz und mögliche Lösungsansätze

Christian Ricardo Kühne

Zusammenfassung

Der Beitrag befasst sich mit dem Datenschutz-Gewährleistungsziel der Transparenz im Kontext hyperkomplexer Verarbeitungen. Dabei geht es um die Frage, wie Betroffene ein hinreichendes Verständnis über die Verarbeitung und ihre Risiken erhalten können, um sie handlungsfähig zu machen. Nach einer kurzen Einführung des Begriffs des Datenschutz-Risikos wird die Verwendung dieses Begriffs für die Risikokommunikation in Richtung Betroffener problematisiert. Anschließend geht der Beitrag auf einige Aspekte menschlicher Wahrnehmung ein und argumentiert, dass die kontextbasierte Verwendung mentaler Konzepte wie Metaphern und Frames in Kombination mit Piktogrammen maßgeblich für die Aktivierung des (individuellen und kollektiven) Risikobewusstseins und -handelns der Betroffenen in der „digitalen" Alltagspraxis sind.

1. Einleitung

Trotz der aktuellen gesetzlichen Pflichten der Europäischen Datenschutz-Grundverordnung (DSGVO) zur Transparenz stehen die von der Verarbeitung betroffenen Personen mehr denn je vor dem alten Problem „hyperkomplexer Systeme" (vgl. Podlech 1982, S. 456), die sich ihnen als *black boxes* darstellen. In der Regel sind die Datenschutzerklärungen mehr ein Feigenblatt als die Bedingung der Möglichkeit zum selbstbestimmten und risikobewussten Handeln (vgl. Kröger u. a. 2021). Die Betroffenen operieren mit vagen Gefühlen und Vorstellungen, die entweder durch mediale Datenschutz- und Sicherheitsskandale geprägt sind oder sich aus Laiengesprächen im Freundes- und Bekanntenkreis speisen.

Bei der Transparenz (Art. 5 Abs. 1 lit. a DSGVO) handelt es sich um eine datenschutzrechtliche Anforderung der DSGVO. Sie ist eine Eigenschaft einer Verarbeitung, die nicht per se existiert, sondern durch zielgerichte-

te Systemgestaltung geschaffen wird und nur durch den Einsatz weiterer Ressourcen aufrecht erhalten werden kann. Die Systemgestaltung obliegt dem operativen Datenschutz, dessen Funktion es ist, die normativen Anforderungen des Rechts in technische und organisatorische Anforderungen zu transformieren und diese in die Gestaltung der Informationsverarbeitung einzubeziehen (vgl. Rost 2017, S. 23 ff). Dazu greift der operative Datenschutz auch auf "Privacy Enhancing Technologies" bzw. datenschutzfreundliche Techniken des Datenschutz-Engineerings zurück (vgl. Bock u. a. 2011). Mit Blick auf die Transparenz ist aus Sicht des operativen Datenschutzes und des Datenschutz-Engineerings die praktische Aufgabe zu lösen, die Verarbeitung entsprechend zu gestalten und ihre Risiken (neben den möglichen Vorteilen) für die Betroffenen verstehbar zu machen und somit eine wesentliche Voraussetzung für Reflexion und Handlungsfähigkeit zu schaffen. Die Diskussionen hierzu beziehen sich unter anderem auf die Erzeugung hinreichend verständlicher Texte und grafischer Darstellungen, mit denen Betroffene bei der Nutzung eines IT-Dienstes oder -Produkts beiläufig in Kontakt kommen (vgl. etwa Effroni u. a. 2019, Grassl 2024). Im Rahmen der Tagung vom 9. und 10. Oktober 2025 am Humboldt-Institut für Internet und Gesellschaft (HIIG) wurde auch die Rolle vorherrschender "Narrative" im Datenschutz beleuchtet und festgestellt, dass sie unter anderem auf den Selbstdatenschutz abstellen und zugleich die realen informationellen Machtverhältnisse verschleiern. Hierzu zählen sicherlich auch neoliberale Erzählungen, die durch die Fixierung auf das Individuum die individuellen Risiken tendenziell stärker in den Vordergrund stellen als die gesellschaftlichen Risiken und eine "organisierte Unverantwortlichkeit" (vgl. Blühdorn 2024, S. 125) entstehen lassen.

Dieser Beitrag erläutert einige Probleme in Bezug auf die Anforderungen der Transparenz und argumentiert, warum die kontextbasierte Verwendung metaphorischer Sprache in Kombination mit Piktogrammen maßgeblich für die Aktivierung des (individuellen und kollektiven) Risikobewusstseins und -handelns der Betroffenen in der "digitalen" Alltagspraxis sind. Hierzu werde ich im ersten Schritt den Risikobegriff aus dem Datenschutz einführen, um anschließend im zweiten Schritt seine Verwendung für die Risikokommunikation zu problematisieren. Im dritten Schritt gehe ich auf die menschliche Wahrnehmung ein und erörtere im letzten Schritt anhand eines Beispiels einige bekannte Lösungsansätze für die Risikokommunikation.

2. Risiken im Datenschutz

Wie werden Risiken im Datenschutz und Datenschutzrecht verstanden? Eine wichtige Referenz bietet das Handbuch zum Standard-Datenschutzmodell (SDM), das von der Konferenz der unabhängigen Aufsichtsbehörden des Bundes und der Länder herausgegeben wurde (s. DSK 2024). Es ist daraufhin konzipiert worden, die rechtlichen Anforderungen der Europäischen Datenschutz-Grundverordnung (DSGVO) in technisch-organisatorische Anforderungen zu übersetzen und sie damit operationalisierbar zu machen. Im Sinne des SDM (und der DSGVO) ist ein Datenschutz-Risiko die Möglichkeit eines Ereignisses, das einen Schaden für natürliche Personen sowie deren Rechte und Freiheiten im Kontext der Verarbeitung personenbeziehbarer Daten darstellt (DSK 2024, S. 49). Allein durch den Umstand, dass diese Daten verarbeitet werden, erzeugt eine Verarbeitung grundsätzlich Risiken für betroffene Personen. Mit anderen Worten: Die Verarbeitung ist an sich bereits riskant.[1] Das SDM differenziert darüber hinaus vier verschiedene Risikotypen, von denen das oben genannte Risiko zum Typ A gehört (ebd., S. 50 f.):

- Risikotyp A: Der Grundrechtseingriff bei natürlichen Personen durch die Verarbeitung ist nicht hinreichend milde gestaltet.
- Risikotyp B: Die Maßnahmen zur Verringerung der Eingriffsintensität einer Verarbeitung sind, in Bezug auf die sieben Gewährleistungsziele des Datenschutzes,[2] nicht vollständig oder werden nicht hinreichend wirksam betrieben oder nicht in einem ausreichenden Maße stetig kontrolliert, geprüft und beurteilt.
- Risikotyp C: Die Maßnahmen, die nach der Informationssicherheit geboten sind (vgl. z. B. IT-Grundschutz des BSI 2017), sind nicht vollständig oder werden nicht hinreichend wirksam betrieben oder werden nicht in einem ausreichenden Maße stetig kontrolliert, geprüft und beurteilt.
- Risikotyp D: Die Maßnahmen der Informationssicherheit werden nicht ausreichend datenschutzgerecht, im Sinne des Risikotyp A und Risikotyp B, betrieben.

1 Diese Einsicht geht auf die Technikfolgenforschung zurück, wonach jede Technik, also auch die IT-gestützte Verarbeitung, trotz ihrer sicheren Gestaltung grundsätzlich ein Risiko wie etwa Freiheitsbeeinträchtigungen für die Betroffenen birgt.

2 Nichtverkettung, Datenminimierung, Transparenz, Intervenierbarkeit, Integrität, Verfügbarkeit, Vertraulichkeit.

Ein Beispiel für Risikotyp A ist die Beeinträchtigung des Rechts auf Nichtdiskriminierung (Art. 21 Charta der Grundrechte der Europäische Union), für Risikotyp B die fehlende Umsetzung eines Löschkonzepts (zur Gewährleistung der Datenminimierung), für Risikotyp C ein materieller Schaden aufgrund eines Identitätsdiebstahls und für Risikotyp D die Protokollierung von personenbezogenen Aktivitäten über das erforderliche Maß hinaus.

Aus Sicht der Systemgestaltung ist die Modellierung von Risiken u. a. aufgrund der Komplexität heutiger Verarbeitungen und moderner Angriffstechniken keine leichte Aufgabe (vgl. Gürses u. a. 2017). Eine Schwierigkeit besteht darin, dass sie einerseits in einer abstrakten Form bestehen können, im Sinne der Beeinträchtigung eines oder mehrerer Grundrechte, was die Bestimmung geeigneter Schutzmaßnahmen erschwert. Anderseits werden Risiken durch eine mehrdimensionale Analyse kleinteiliger und konkretisierbar für die Praxis, was aber zugleich die Komplexität im Risikomanagement erhöht. Die letztgenannte Analyse von Risiken beinhaltet unter anderem die Dimensionen Risikoquelle, Schwachstelle, betroffenes Schutzgut (Person/Recht/Schutzziel), Risikoszenario sowie Eintrittswahrscheinlichkeit und Schwere, aus denen sich eine Gesamtbewertung ergibt (vgl. Friedewald u. a. 2017, S. 28 ff.).

3. Das Problem des Risikobegriffs

Der oben entfaltete Begriff des Datenschutz-Risikos ist allerdings in mehrfacher Hinsicht problematisch, wenn es darum gehen soll, die Betroffenen über die Verarbeitung und ihre Datenschutz-Risiken zu informieren, um sie handlungsfähig zu machen.

Die Verrechtlichung des Datenschutzes und die Dominanz rechtlichen Denkens in der Datenschutzpraxis hatten unter anderem zur Folge, dass in einem Teil des europäischen Datenschutzdiskurses eine bestimmte Idee wirkmächtig geworden ist: Datenschutz ist Grundrechteschutz. Dahinter steht die Vorstellung, dass die verfassungsrechtlichen Normen, wozu auch die Grundrechte gehören, als normatives Fundament für Demokratie, Rechtsstaatlichkeit, individuelle Freiheit usw. in allen Sphären der Gesellschaft zu verwirklichen seien, und zwar auch im sogenannten "Informationsbereich". Die Pioniere des Datenschutzes begründen die normative Idee des Datenschutzes auf der Verfassung, denn "[n]ur sie nimmt als zentraler

Bezugspunkt auf unser ganzes Leben Einfluss" (vgl. Steinmüller u. a. 1971, S. 60). An dieser Idee sollten wir weiterhin festhalten. Gleichwohl sind aus soziologischer Sicht kommunikative Verwerfungen erwartbar, wenn sie unmittelbar für die Risikokommunikation mit Betroffenen verwendet wird. "Risiken für die Rechte und Freiheiten"[3] sind für Betroffene nur schwer vermittelbar. Ein wesentlicher Grund dafür ist, dass Menschen, die keine Erfahrung mit der Verletzung eines oder mehrerer ihrer Grundrechte und ihrer Verteidigung haben, nur eine sehr vage Vorstellung von "ihren" Grundrechten haben, wie sie etwa im deutschen Grundgesetz oder in der Charta der Grundrechte der Europäischen Union niedergelegt sind (vgl. FRA 2024, S. 59).

Das zweite Problem in Bezug auf die Kommunikation von Datenschutz-Risiken besteht darin, dass die datenverarbeitenden Organisationen (mit Ausnahme von Fällen der internationalen Datenübermittlung nach Art. 49 Abs. 1 lit. a DSGVO) keiner gesetzlichen Pflicht unterliegen, die Risiken und Schutzmaßnahmen gegenüber den Betroffenen zu beschreiben. Diese Information bleibt einzig den Organisationen selbst und den Datenschutzaufsichtsbehörden zur Prüfung vorbehalten.

Das dritte Problem besteht hinsichtlich der Form der bereitgestellten Informationen zur Einhaltung der Transparenzpflichten. Hierbei spielt die Datenschutzerklärung eine zentrale Rolle, dessen Funktion in erster Linie darin besteht, über die Verarbeitung und die Verantwortlichkeit aufzuklären. Zur charakteristischen Form von Datenschutzerklärungen im Internet gehört ihre erdrückende Textlänge, die Verwendung juristischer Fachsprache und nicht zuletzt die generische Beschreibung, die keinen Bezug zu konkreten Verarbeitungen erkennen lässt (vgl. auch Kröger u. a. 2021). Der Zusammenhang zwischen der rechtlichen Anforderung der Transparenz und seiner praktischen Umsetzung wirkt geradezu paradox: Die Anforderung der Transparenz wird gewissermaßen durch "intransparente" (unverständliche, lange, ungenaue) Texte umgesetzt. Der Grund dafür liegt meines Erachtens in der Dominanz rechtlichen Denkens innerhalb der Datenschutzpraxis, mit der Folge, dass andere Kommunikationsformen als die juristische Fachsprache nicht zum Zuge kommen. Die ergänzende Beschreibung von Datenschutz-Risiken dürfte wohl noch mehr Öl ins Feuer gießen. Auf Seiten der Betroffenen als Adressaten dieser Kommunikation besteht hingegen tendenziell ein Mangel an Zeit und ggf. kognitiver Kapazitäten

3 Diese und ähnliche Formulierungen finden sich unter anderem in Art. 24, 25, 32, 35 DSGVO.

zur Verarbeitung der dargebotenen Informationen (ebd.). Diese Erkenntnis ist nicht neu und spiegelt sich in verschiedenen Maßnahmenempfehlungen des operativen Datenschutzes und des Datenschutz-Engineerings wider (siehe dazu Abschnitt 5).

4. Menschliche Wahrnehmung als Ausgangspunkt

Doch was wäre zu berücksichtigen, um das Verständnis über die Verarbeitung und die Abwägung von möglichen Vorteilen und Risiken zu erleichtern und die Betroffenen handlungsfähig zu machen? Um der Beantwortung dieser Frage ein Stück näherzukommen, lohnt es sich, einige Erkenntnisse der Sprach- und Kognitionswissenschaften zur Frage heranzuziehen, wie Menschen denken und wahrnehmen. Danach ist bekannt, dass das menschliche Denken größtenteils unbewusst geschieht und tiefgreifend von Metaphern und Deutungsrahmen geprägt ist (vgl. Lakoff u. a. 2016, S. 14). Menschen sind im Allgemeinen wenig empfänglich für Fakten und Zahlen. In Bezug auf das Beispiel der politischen Wahlen in den USA sei es ein Irrglaube, so der Kognitionswissenschaftler George Lakoff, dass Menschen auf Basis von Fakten wählen, sie tun dies in der Hauptsache durch mentale Konzepte wie Metaphern, die auf sozialen Erfahrungen und moralischen Werten basieren (vgl. ebd. S. 71).[4] Die Erkenntnis um die fragile Wirkung von Fakten hingegen lässt sich meines Erachtens auch auf das oben genannte Negativbeispiel typischer Datenschutzerklärungen oder die Idee, "Risiken für die Rechte und Freiheiten" im Kontext der Risikokommunikation zu thematisieren, beziehen. Wenn einerseits nur „rechtliche Tatsachen" (hier: die mögliche Beeinträchtigung von Rechten) thematisiert werden und andererseits die Annahme über die fragile Wirkung von Fakten stimmt, so lässt sich schlussfolgern, dass ihre zweckmäßige Wirkung aller Voraussicht nach ausbleiben wird – wobei dies nicht bedeutet, dass Fakten keine Bedeutung haben, sondern dass sie sinnvoll eingesetzt werden sollten, z. B. als Grundlage für die visuelle Kommunikation.

4 Zu diesen sozialen Erfahrungen gehören räumliche Erfahrungen (z. B. oben und unten), gegenständliche Erfahrungen (z. B. Fassen und Greifen), familiäre Erfahrungen (z. B. Geborgenheit, Fürsorge oder Strenge), Erfahrungen zur Haushaltsführung (z. B. Einkommen, Vorsorge und Verzicht) oder Kriegserfahrungen. Dabei sind einige der Erfahrungen aus dem Alltagsleben moralisch konnotiert: Ein guter Haushalt ist ein ausgeglichener Haushalt, eine gute Mutter ist eine fürsorgliche Mutter und so weiter.

Metaphern hingegen ermöglichen es den Menschen, mit abstrakten oder unbekannten Begriffen schneller und effektiver umzugehen, indem wir etwa eine Theorie als Gebäude verstehen (vgl. ebd. S. 22 f.). Ihre Funktion besteht darin, den Sinn von einem Sinnbereich in einen anderen zu übertragen. Dabei heben Metaphern bestimmte Aspekte hervor und verstecken andere. Eine Theorie hat so gesehen Axiome, die das "Fundament" bilden und Thesen, die durch entsprechende Argumente "untermauert" werden müssen (vgl. Lakoff u. a. 2018, S. 59).

Wörter können zudem einen Deutungsrahmen (engl. "Frame") induzieren, also eine Kette von Assoziationen ein- und dadurch andere mögliche Deutungen ausblenden (vgl. Lakoff u. a. 2016, S. 28). Ein Ereignis kann als Explosion, Bombenanschlag oder Terrorangriff gerahmt werden, wodurch die Perspektive auf den Sachverhalt verändert wird. Frames ermöglichen daher, das Denken in bestimmte Bahnen zu lenken.

Ein wichtiges Framing bei der Kommunikation von möglichen Vorteilen und Risiken im Kontext von Verarbeitungen geschieht bereits bei der Zwecksetzung. Sie kann bereits Andeutungen darüber enthalten, was die zu erwartenden Vorteile, aber auch Risiken der Verarbeitung sind. Ein plakatives Beispiel ist der Zweck der "Online-Durchsuchung", der eher die verbesserte Polizeiarbeit bei der Kriminalitätsbekämpfung als Vorteil hervorhebt, wohingegen der Zweck der "Staatstrojanisierung" wohl eher die Risiken von Schadsoftware und staatlicher Kontrolle ins Gedächtnis ruft.

Analogien haben eine ähnliche Wirkung wie Metaphern, denn sie ermöglichen das Erschließen von Unbekanntem aus Bekanntem aufgrund von Struktur- oder Funktionsähnlichkeiten. Eine gute Analogie setzt allerdings voraus, dass diese Gleichheit von Strukturmerkmalen und Verhältnissen zuvor geprüft wurde, um sie richtig zum Einsatz bringen zu können.[5]

Ein anderes komplexeres mentales Konzept sind Narrative, also sozial wirkmächtige Erzählungen. Als solche machen sie Sinnhaftes für die Menschen überhaupt erst zugänglich (vgl. Meuter 2008, S. 400). Indem sie etwas beschreiben, das den Menschen widerfahren ist, ermöglichen sie es anderen, die erlebten Konsequenzen nachzuvollziehen (vgl. Herman 2007, S. 3). Ein Beispiel hierfür sind die wiederkehrenden Erzählungen über sogenannte künstliche Intelligenz (KI), in denen die Menschen ihre Erfahrungen über das eigenständige "Agieren" und "Entscheiden" von KI-Systemen teilen und dadurch die Vorstellung des autonomen Handelns

5 Jörg Pohle hat diesen Gedanken auf der Tagung vorgetragen und dafür plädiert, die Strukturgleichheit von Analogien zu prüfen und nachzuweisen.

solcher Systeme sozial festigen und dadurch einfacher abrufbar machen, unabhängig von ihrem Wahrheitsgehalt (vgl. Rehak 2023). Im Gegensatz zu Metaphern und Analogien sind sie allerdings deutlich aufwendiger für die Thematisierung von Risiken in Stellung zu bringen. Ich stelle mir Folgendes darunter vor: Damit ein Narrativ funktioniert, bedarf es eines (performativen) Akts wie dem Erzählen oder dem Lesen einer Erzählung, um das Narrativ zur Entfaltung zu bringen. In ihrer klassischen Form hat eine Erzählung einen Anfang, eine Mitte und einen Schluss. Damit betroffene Personen die Erzählung nachempfinden können, bedarf es zudem einer Protagonistin. Die Erzählung beginnt mit der Ausgangssituation einer scheinbar harmlosen Verarbeitung, aus der heraus die Protagonistin ggf. einen Konflikt oder ein besonderes Ereignis erlebt. Auch Emotionen wie Angst oder Wut aufgrund von unerwünschten Folgen einer Verarbeitung spielen dabei eine wichtige Rolle, da die Erzählung sonst nicht verfängt. Die Erzählung bzw. das Risikonarrativ endet mit einer geschädigten Person, Gruppe oder Gesellschaft. Je bekannter und gefestigter das Narrativ im kollektiven Gedächtnis ist, desto kürzer darf die Beschreibung ausfallen. Der Skandal von Cambridge Analytica wurde vielleicht oft genug erzählt, um lediglich vom „Missbrauch psychometrischer Daten für die Einflussnahme auf politische Wahlen" als Risikonarrativ zu sprechen. Vielleicht ist der Skandal auch schon vergessen und muss in angemessener Breite (performativ) neu erzählt werden.

5. Konstruktive Vorschläge zur Kommunikation von Risiken im Datenschutz

Relevant für die Datenschutzpraxis ist nun, dass sich das Wissen um diese kognitiven Mechanismen konstruktiv und im Interesse der Betroffenen einsetzen lässt.[6] Allerdings ist die Suche nach geeigneten Metaphern, Frames, Analogien und Narrativen keine einfache Aufgabe, die Ergebnisse und ihre Wirkung sollten meines Erachtens mit Usability-Tests bzw. empirischen Experimenten nachgeprüft werden.

6 Der Unterschied zur Propaganda oder dem politischen Spin besteht darin, dass diese bewusst Unwahrheiten vermitteln sollen, um politische Kontrolle zu erlangen. Vgl. Lakoff u. a. 2016, S. 85 f.

Illustrieren möchte ich dies anhand einer Beispielverarbeitung, die dem Zweck dient, innerhalb des Europäischen Wirtschaftsraums elektronisch zu bezahlen.[7] Die Verarbeitung umfasst unter anderem

- das Verfahren und seine Verarbeitungsvorgänge (Anmeldung, Kontoeinrichtung, Zahlungen durchführen, Vertragsende),
- die zugehörige Aufbau- und Ablauforganisation,
- die Server,
- die App (für das Smartphone),
- die Kommunikationsverbindungen und vieles mehr.

Informationen zu datenschutzspezifischen Aspekten der Verarbeitung sollten nach Stand der Technik so gestaltet sein, dass diese den Betroffenen situationsbezogen (also z. B. zum Zeitpunkt der Datenerhebung oder Verwendung einer neuen Funktion) und ihrem Informationsbedarf entsprechend bereitgestellt werden.[8] Zudem sollten die Informationen auf zwei bis drei Informationsstufen unterschiedlich detailliert aufbereitet sein.[9] Informationen auf der ersten Stufe sollen dazu dienen, Kerninformationen wie Zwecke und Mittel in kurzer Zeit zu erfassen. Hier helfen auch Datenschutz-Symbole, die Informationen schneller als Text zu vermitteln. Durch weitere Klicks erhalten Betroffene auf der zweiten Stufe beispielsweise Kurzmitteilungen zu Informationen nach Art. 13 DSGVO, während auf der dritten Stufe die vollständigen Informationen dargestellt sind.

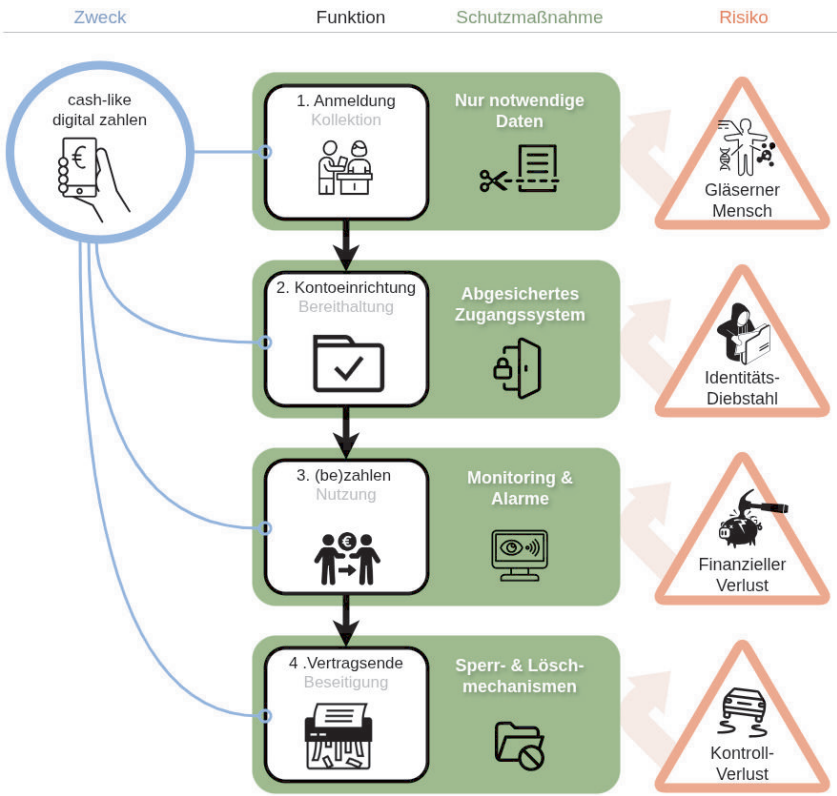
Abbildung 1 zeigt eine Versuchsskizze für eine Info-Grafik, wie sie auf der ersten Stufe (zum Zeitpunkt der Datenerhebung) zum Einsatz kommen könnte. Bitte schauen Sie sich diese für etwa zehn Sekunden an und vergleichen Sie Ihren ersten Eindruck mit der nachfolgend beschriebenen Gestaltungsabsicht.

7 Siehe dazu beispielhaft das aktuelle Vorhaben der Europäischen Zentralbank, einen digitalen Euro als elektronisches Zahlungsmittel einzuführen. Abrufbar unter: https://www.ecb.europa.eu/euro/digital_euro/html/index.de.html.

8 Siehe hierzu die Mustersprache des Projektes "Privacy by Design" zur Strategie "Informieren". Abrufbar unter: https://privacybydesign.digital.

9 Ebd.

Abbildung 1: Datenschutzinformation als Kurzmitteilung (erste Informationsstufe) zum Zeitpunkt der Erhebung (Vorschlag/ Entwurf).



Die unterschiedlichen Elemente und Gestaltungsentscheidungen sollen kurz beschrieben werden. Insgesamt werden drei Kerninformationen dargestellt: (1) der Zweck der Verarbeitung, (2) die wesentlichen Funktionen sowie (3) die Primär-Risiken und -Schutzmaßnahmen. Als Primär-Risiko bezeichne ich ein hohes Risiko vom Typ A oder B (im oben genannten Sinne des SDM) und als Primär-Schutzmaßnahme die stärkste Schutzmaßnahme nach Stand der Technik, mit der einem solchen Risiko begegnet

wurde.[10] Den Lesegewohnheiten entsprechend, beginnt die Darstellung links mit dem Zweck. Der Zweck, "digital zu bezahlen", enthält bereits durch das zusätzliche Wort "cash-like" ein bestimmtes Framing, das vielleicht den Gedanken des *anonymen* Zahlens aufkommen lässt. Aus dem Zweck leiten sich die wesentlichen Funktionen ab, die zugleich den Phasen einer Verarbeitung aus Datenschutzsicht entsprechen (vgl. DSK 2024, S. 38). Auf diese Weise kann der Überraschungseffekt für Betroffene reduziert und der Erwartungshorizont erweitert werden. Die Kunst besteht darin, einen Weg zwischen einer übermäßigen Vereinfachung und Verkomplizierung zu finden. Eng verknüpft mit den Funktionen ist das jeweilige Primär-Risiko und der entsprechende Primär-Schutz. Die notwendige Grundlage hierfür ist eine zuvor erstellte Risikobetrachtung bzw. Datenschutz-Folgenabschätzung (DSFA).[11] Aus einer solchen DSFA geht aller Voraussicht nach hervor, dass hier andere, möglicherweise ebenso schwerwiegende Risiken vorhanden sind. Doch auch hier denke ich, dass für das konkrete Gestaltungsziel gelten sollte: weniger ist mehr. Die Auswahl der Primär-Risiken könnte bspw. durch interne Datenschutzbeauftragte oder Betroffene erfolgen (vgl. Art. 35 Abs. 9 DSGVO). Die Fokussierung auf sogenannte Primär-Risiken beabsichtigt, zwei Wirkungen bei den Betroffenen auszulösen: erstens das Risikobewusstsein innerhalb der Aufmerksamkeitsspanne von zehn Sekunden zu wecken und zweitens zu einer ersten persönlichen Einschätzung der *relevanten* kontextspezifischen Risiken zu drängen. Unter den vier Risiken finden sich drei aus der DSGVO entnommene Schadensszenarien, nämlich Identitätsdiebstahl, finanzieller Verlust und Kontrollverlust über die verarbeiteten Daten.[12] Dabei kann sich das Risiko des Identitätsdiebstahls aus der Unsicherheit der Verarbeitung und seiner Ausnutzung durch externe Angreifer ergeben. Aufgrund der einseitig vermachteten Verarbeitung kann sich ein finanzieller Verlust oder auch Kontrollverlust über das Bankkonto ergeben, indem die kontoführende Bank Transaktionen manipuliert oder das Konto aufkündigt. Für alle Primär-Risiken wurden metaphorische Titel und/oder Piktogramme gewählt, um den Sinn aus der Erfahrungswelt der Betroffenen in den Kontext der Verarbeitung zu übertragen (z. B. durch Gespräche und Usability-Tests).

10 Die Zuordnung von Risiko und Schutzmaßnahme ist hier als idealisiertes 1:1-Verhältnis dargestellt. Bei näherer Betrachtung kommt es vor, dass für ein Risiko verschiedene Schutzmaßnahmen erforderlich oder aber mehrere Risiken von einer Schutzmaßnahme abgedeckt sind.

11 Siehe dazu unter anderem Friedewald u. a. 2017.

12 Siehe Erwägungsgrund 75 der DSGVO.

Beispielsweise ergibt sich aus der Metapher "Identität ist Eigentum", dass Identitäten auch gestohlen werden können. Durch die Metapher "Daten sind Steuergeräte" ergibt sich der übertragene Sinn, seine Geschäfte steuern zu können oder aber die Kontrolle zu verlieren und ins finanzielle "Schleudern" zu geraten. Die Darstellung der Risiken wird zusätzlich durch das typische Symbol eines Verkehrswarnschildes unterstützt.

Alle dargestellten Risiken stellen mehr oder weniger Risiken für das Individuum dar. Auf der anderen Seite ist die Thematisierung struktureller Datenschutz-Risiken von größerer politischer Bedeutung. Allerdings scheinen diese nach meinem Eindruck eher belanglos für (individuelle) Betroffene zu sein, sofern sie nicht medial skandalisiert wurden. In einer weitestgehend individualisierten Gesellschaft überwiegen die Einzigartigkeit und das Eigeninteresse gegenüber der Allgemeinheit (vgl. Reckwitz 2017 S. 434 ff.). Überschreitet eine Verarbeitung aufgrund seines großen Umfangs oder der großen Anzahl von Betroffenen die Schwelle der medialen Aufmerksamkeit, kann ein öffentliches Interesse an strukturellen Risiken entstehen (wie etwa im Falle des „Digitalen Euros" und der Forderung des anonymen Zahlens). Abbildung 2 zeigt daher eine Variante in Bezug auf den Bezahlvorgang, bei der das Primär-Risiko die Überwachung und anschließende soziale Kontrolle mithilfe der Finanztransaktionsdaten eines Großteils der Gesellschaft ist. Aus den Finanzinformationen lassen sich beispielsweise Informationen über das gewerkschaftliche oder politische Engagement, Konsumverhalten oder Krankheiten von Individuen, Gruppen oder sozialen Bewegungen ableiten, die vom Verantwortlichen oder sonstigen staatlichen Organisationen für andere illegitime Zwecke missbraucht werden können (vgl. DLF 2025).

Abbildung 2: Variante mit Darstellung eines strukturellen Primär-Risikos und -Schutzes.

Bei der Gestaltung sind auch die Grenzen von Metaphern, Analogie und Frames im Blick zu behalten, auf die ich aus Platzgründen nicht näher

eingehen kann: Einige Metaphern wie "Liebe als Hitze" sind nach Lakoff/Wehling (2016, S. 25) universell, andere hingegen wie zum Beispiel "Liebe als gemeinsame Reise" oder der "Mensch als Glas" (und seine Ableitung "gläserne Person") sind kulturabhängig.

6. Schluss

Die Risikokommunikation von Organisationen zu Betroffenen ist heutzutage größtenteils unterentwickelt und geschieht nahezu ausschließlich organisationsintern im Rahmen des Datenschutz- bzw. Risiko-Managements. Dies ist vor allem auf die datenschutzrechtlichen Mindestanforderungen aus Art. 13 ff. DSGVO zurückzuführen. Zwei Hindernisse stehen einer betroffenengerechten Risikokommunikation auf den ersten Blick entgegen: Zum einen schreibt Art. 32 DSGVO vor, dass ein den Risiken angemessenes Schutzniveau bereits zum Zeitpunkt der Inbetriebnahme vorhanden sein muss, sodass aus Organisationssicht in der Theorie keine relevanten Risiken mehr bestehen, auf die ggf. hinzuweisen wären. Zweitens haben Organisationen im Wirtschaftsbereich aufgrund der Konkurrenzlogik kein genuines Interesse daran, die ggf. auch nur abstrakten Risiken ohne weiteres öffentlich zu thematisieren, da hierdurch aller Voraussicht nach ein wirtschaftlicher Nachteil entsteht. Ein möglicher Ausweg könnte gemäß der oben skizzierten Info-Grafik daher darin bestehen, zusätzlich zu den Risiken die getroffenen Schutzmaßnahmen zu thematisieren, um sie als "besondere Qualität" im Wettbewerb hervorzuheben.[13] Die Plausibilität der Risikobetrachtung und die Wirksamkeit der getroffenen Maßnahmen ließe sich wiederum durch Vergleiche ähnlicher Verarbeitungstätigkeiten oder durch eine unabhängige Zertifizierungsstelle prüfen und durch eine entsprechende Datenschutz-Zertifizierung nachweisen (vgl. Art. 42 DSGVO). Der oben skizzierten Ansatz ist nicht neu, sondern verwendet Gestaltungselemente, die dem Stand der Technik entsprechen. Die Betroffenen können sich so einerseits ein Bild von den Anstrengungen der Organisation machen und andererseits erste Risikoabwägungen vornehmen, um ggf. ihr Verhalten anzupassen.

Die Gestaltung einer bedarfsgerechten und effektiven Chancen- und Risikokommunikation im Interesse der Betroffenen ist eine anspruchsvol-

13 Siehe zum Beispiel den Mail-Provider Posteo, der mit seinen implementierten Datenschutzmaßnahmen wirbt. Abrufbar unter https://posteo.de/site/leistung.

le Aufgabe innerhalb einer Organisation, die unter Umständen mehrere Iterationen mit User-Feedback und (je nach Reifegrad der Organisation) ein interdisziplinäres Team aus Kommunikations-Designer:innen, Informatiker:innen und Jurist:innen benötigt. Neben den Datenschutz-Anforderungen werden weitere Anforderungen wie etwa die Barrierefreiheit oder die Wirtschaftlichkeit in Einklang zu bringen sein. Doch die heutigen Gestaltungstechniken für das Kommunikationsdesign bieten vielfältige und kostengünstige Möglichkeiten wie den Einsatz von Tooltips (HTML5), Piktogrammen und sprachlichen Metaphern.

Credits

Vielen Dank an das Noun-Project[14] und seine Künstler:innen, die mir die Nutzung der Piktogramme unter der CC BY-3.0 Attribution License erlauben: “monitoring”, created by Eko Purnomo; “Folder”, created by Ilham Fitrotul Hayat; “Stability Control”, created by LAFS; “transaction”, created by Alice Design; “smartphone payment”, created by Eliricon; “data hacker”, created by Azam Ishaq; “piggybank broken”, created by b farias; “shredder”, created by Eliricon; “body scan”, created by Mexicons; “lock door”, created by Gregor Cresnar; “money”, created by Putri Creative; “surveillance”, created by RanuKumbolo.Lab; “cutting”, created by Adrien Coquet; “checkin”, created by khoiryah; “Check Folder”, created by kitaicons.

Literatur

Blühdorn, Ingolfur (2024): Unhaltbarkeit. Auf dem Weg in eine andere Moderne. Berlin: Suhrkamp.

Bock, Kirsten und Rost, Martin (2011): *Privacy by Design und die Neuen Schutzziele. Grundsätze, Ziele und Anforderungen.* Datenschutz und Datensicherheit, 1, S. 30–35.

BSI (2017): BSI-Standard 200-2. IT-Grundschutz-Methodik. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html (besucht am 21.02.2026).

DLF (2025): Supreme Court gewährt Doge Zugriff auf Daten der Sozialversicherung. URL: https://www.deutschlandfunk.de/supreme-court-gewaehrt-doge-zugriff-auf-daten-der-sozialversicherung-100.html (besucht am 22.02.2026).

DSK (2024): *Das Standard-Datenschutzmodell. Eine Methode zur Datenschutzberatung und -Prüfung auf der Basis einheitlicher Gewährleistungsziele. Version 3.1.* URL: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/ (besucht am 19.12.2025).

14 The Noun Project. Abrufbar unter: https://thenounproject.com.

Efroni, Zohar; Metzger, Jakob; Mischau, Lena; Schirmbeck, Marie (2019): Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing. European Data Protection Law Review, 3, S. 352–366.

FRA (2024): GDPR in practice – Experiences of data protection authorities. URL: https://fra.europa.eu/en/publication/print/pdf/node/45346 (besucht am 21.02.26).

Friedewald, Michael; Bieker, Felix; Obersteller, Hannah; Nebel, Maxi; Martin, Nicholas; Rost, Martin und Hansen, Marit (2017): *White Paper Datenschutz-Folgenabschätzung. Ein Werkzeug für einen besseren Datenschutz*. 3. Auflage. URL: https://www.forum-privatheit.de/wp-content/uploads/Forum_Privatheit_White_Paper_DSFA-3.pdf (besucht am 19.12.2025).

Herman, David (2007): Introduction. In: David Herman (Hg.): *The Cambridge Companion to Narrative*. Cambridge: Cambridge University Press, S. 3–21.

Grassl, Paul; Gerber, Nina; von Grafenstein, Max (2024): How Effectively Do Consent Notices Inform Users About the Risks to Their Fundamental Rights? European Data Protection Law Review, 1, S. 96–104. DOI: https://doi.org/10.21552/edpl/2024/1/14.

Gürses, Seda und van Hoboken, Joris (2017): Privacy after the Agile Turn. In: Jules Polonetsky; Omer Tene; Evan Selinger (Hg.): Cambridge Handbook of Consumer Privacy, S. 579–601. DOI: https://doi.org/10.1017/9781316831960.032.

Kröger, Jacob Leon; Lutz, Otto Hans-Martin und Ullrich, Stefan (2021): The Myth of Individual Control: Mapping the Limitations of Privacy Self-management. *SSRN*. DOI: https://doi.org/http://dx.doi.org/10.2139/ssrn.3881776.

Lakoff, George und Wehling, Elisabeth (2016): *Auf leisen Sohlen ins Gehirn. Politische Sprache und ihre heimliche Macht.* 4. Auflage. Heidelberg: Carl-Auer Verlag.

Lakoff, George und Johnson, Mark (2018): *Leben in Metaphern. Konstruktion und Gebrauch von Sprachbildern.* 9. Auflage. Heidelberg: Carl-Auer Verlag.

Meuter, Norbert (2008): Narrativität. In: Peter Prechtl und Frans-Peter Burkard (Hg.): *Metzler Lexikon Philosophie. Begriffe und Definitionen.* 3. Auflage. Berlin Heidelberg: Springer, S. 400–401. DOI: https://doi.org/10.1007/978-3-476-05469-2.

Podlech, Adalbert (1982): Individualdatenschutz – Systemdatenschutz. In: Klaus Brückner und Dalichau Gerhard (Hg.): *Beiträge zum Sozialrecht - Festgabe für Grüner*. Verlag R. S. Schulz, S. 451–462.

Reckwitz, Andreas (2017): *Die Gesellschaft der Singularitäten. Zum Strukturwandel der Moderne*. Berlin: Suhrkamp Verlag.

Rehak, Rainer (2023): Zwischen Macht und Mythos. Eine kritische Einordnung aktueller KI-Narrative. *Soziopolis*. URL: https://nbn-resolving.org/urn:nbn:de:0168-ssoar-91379-4.

Rost, Martin (2017): Organisationen grundrechtskonform mit dem Standard-Datenschutzmodell gestalten. In: Alexandra Sowa (Hg.): *IT-Prüfungen, Sicherheitsaudit und Datenschutzmodell. Neue Ansätze für die IT-Revision.* Wiesbaden: Springer, S. 23–56.

Steinmüller, Wilhelm; Lutterbeck, B.; Mallmann, C.; Harbort, U.; Kolb, G. und Schneider, J. (1971): Grundfragen des Datenschutzes. Gutachten im Auftrag des Bundesministeriums des Innern. In: *BT 72*. Bundesministerium des Innern.

Über den Autor

Christian Ricardo Kühne
studierte Philosophie, Informatik und Soziologie an der HU Berlin. Er ist Referent bei der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI) und forscht an der Schnittstelle zwischen Commons-Theorie und kritischer Informatik zu herrschaftsfreien Informationssystemen. Der Inhalt dieses Beitrags spiegelt nicht die Sichtweise der BlnBDI wider. E-Mail: christian.kuehne@datenschutz-berlin.de.