

BvD-NEWS

Fachmagazin für Datenschutzbeauftragte

Seite 6

INNOVATION MIT SICHERHEITSGURT

Regina Mühlich

Seite 22

TRUMP V. SLAUGHTER: DER TRANSATLANTISCHE DATENTRANSFER

Tim Wybitul

Seite 30

AI BRAIN FRY ALS GRENZE MENSCHLICHER KI-AUFSICHT

Stephan Rehfeld

Berufsverband der
Datenschutzbeauftragten
Deutschlands (BvD) e.V.



mastodon.social/@bvd@privacyofficers.social



linkedin.com/company/berufsverband-der-datenschutzbeauftragten

BvD^{e.V.}

DATENSCHUTZ GESTALTEN



INNOVATION MIT SICHERHEITSGURT

Warum Vertrauen aus guten Entscheidungen entsteht

Regina Mühlich

In der Praxis scheitert Innovation selten an fehlender Technik. Weitaus häufiger fehlen Akzeptanz, Nachvollziehbarkeit und Vertrauen. Der Beitrag zeigt, warum Datenschutz gerade in Innovations- und Transformationsprojekten nicht als Bremse, sondern als belastbarer Sicherheitsgurt verstanden werden sollte und warum Entscheidungsklarheit, Risikoklarheit sowie Kommunikationsklarheit die eigentlichen Voraussetzungen dafür sind, dass Innovation im Alltag tragfähig wird.

Wenn über Innovation gesprochen wird, richtet sich der Blick fast reflexhaft auf Technologie, auf Künstliche Intelligenz, Automatisierung, neue Plattformen, neue Fachverfahren, neue Tools. Die zugrunde liegende Annahme ist weit verbreitet, aber auch verkürzt: Wenn die Technik leistungsfähig genug ist, wird der Rest schon folgen. Genau das ist in der Praxis aber häufig nicht der Fall.

Denn selten scheitert Innovation an technischen Möglichkeiten. Sie scheitert oft an einem Mangel an Orientierung. An fehlender Zuständigkeit. An unklaren oder fehlenden

Prozessen. An offenen Schnittstellen. Und vor allem an etwas, das sich später nicht einfach „nachinstallieren“ lässt: Vertrauen. Die eigentliche Herausforderung liegt daher oft nicht in der Frage, ob etwas technisch möglich ist. Sie liegt darin, wie etwas eingeführt wird, damit es nachvollziehbar, vertretbar und tragfähig bleibt. Genau hier beginnt der eigentliche Beitrag des Datenschutzes.

Datenschutz ist in solchen Konstellationen keine Störung im System. Er ist auch nicht der moralische Zeigefinger am Rand des Projekts. Und er ist erst recht nicht bloß eine formale Freigabeschleife am Ende eines bereits weitgehend entschiedenen Vorhabens. Vielmehr ist Datenschutz der Rahmen, der Innovation belastbar macht. Oder, um es zugespitzt zu formulieren: Datenschutz ist der Sicherheitsgurt der Innovation.

Dieses Bild ist deshalb so treffend, weil ein Sicherheitsgurt nicht das Fahren verhindern soll. Er ist auch kein Ausdruck von Misstrauen gegenüber dem Fahrzeug oder dem Ziel.

Er soll dafür sorgen, dass man fahren kann, ohne dass aus Fehlern, Unklarheiten oder Fehlentscheidungen unmittelbar Schaden entsteht. Übertragen auf Organisationen bedeutet das: Datenschutz soll Innovation nicht blockieren, er soll sie so absichern, dass sie verantwortbar bleibt – auch unter Zeitdruck, bei knappen Ressourcen und wenn Projekte mit dem bekannten Satz beginnen: „Kannst du mal eben draufschauen?“.

Vertrauen ist keine Stimmung, sondern Infrastruktur

In vielen Projekten trifft man auf gute Absichten. Diese klingen zunächst vernünftig, pragmatisch und lösungsorientiert. „Das ist doch nur ein Pilot.“ „Wir machen das erstmal schnell.“ „Datenschutz klären wir später.“ Besonders beliebt ist auch der Klassiker: „Wir speichern das nur kurz.“ Solche Sätze sind nicht ungewöhnlich. Sie schaffen oft sogar Aufbruchsstimmung. Was sie jedoch nicht schaffen ist Struktur.

Gerade darin liegt ein weitverbreitetes Missverständnis. Vertrauen entsteht nicht allein dadurch, dass die Beteiligten es gut meinen. Auch durch optimistische Projektkommunikation oder die Hoffnung, dass sich kritische Punkte später schon auflösen werden, entsteht kein Vertrauen.

Vertrauen entsteht, wenn Verantwortliche nachvollziehbar erklären können, was mit Daten geschieht, warum es geschieht, wer dafür zuständig ist und welche Grenzen dabei gelten. Es entsteht dort, wo Betroffene, Mitarbeitende, das Management und notfalls auch die Öffentlichkeit nachvollziehen können, dass ein Vorhaben nicht nur innovativ, sondern auch verantwortungsvoll ausgestaltet ist.

Deshalb ist Vertrauen in Organisationen keine weiche Kategorie. Es ist kein atmosphärischer Zusatznutzen und kein Kommunikationsornament. Vertrauen ist Infrastruktur.



Es trägt Prozesse, Entscheidungen und Akzeptanz. Fehlt diese Infrastruktur, wird auch das technisch überzeugendste Projekt schnell fragil. Dann kippt ein Vorhaben nicht zwingend aufgrund seiner Funktionalität, sondern aufgrund offener Fragen, unklarer Verantwortlichkeiten oder fehlender Erklärbarkeit.

Für Datenschutzbeauftragte ist das eine zentrale Botschaft. Ihre Aufgabe besteht nicht darin, am Rande eines Projekts Warningschilder aufzustellen. Ihre eigentliche Stärke liegt darin, aus guten Absichten belastbare Entscheidungsgrundlagen zu schaffen. Sie übersetzen Unsicherheit in Struktur. Und genau dadurch leisten sie einen wesentlichen Beitrag dazu, Innovationsprojekte umsetzbar zu machen.

Drei Klarheiten, die Vertrauen tragfähig machen

Ein besonders praxistauglicher Zugang besteht darin, Innovationsprojekte entlang von drei Formen der Klarheit zu betrachten: Entscheidungsklarheit, Risikoklarheit und Kommunikationsklarheit. Diese drei Ebenen bilden zusammen so etwas wie das Dreipunktgurt-System der Innovation. Sind sie vorhanden, entsteht Vertrauen nicht zufällig, sondern als Ergebnis guter Entscheidungen.

1. Entscheidungsklarheit: Wer entscheidet was – und warum?

Viele Projekte starten mit einer Mischung aus Erwartungsdruck, technischem Interesse und dem nachvollziehbaren Wunsch, „endlich etwas zu machen“. Nicht selten stehen am Anfang Formulierungen wie: „Wir müssen digitaler werden.“ „Wir wollen innovativ sein.“ oder „Die anderen machen das auch.“ All das kann ein legitimer Anlass sein, aber noch keine belastbare Entscheidung.

Entscheidungsklarheit beginnt deshalb mit einer schlichten, aber oft erstaunlich anspruchsvollen Frage: „Was ist der Zweck?“ In einem Satz. Wenn sich ein Innovationsvorhaben nicht in einem klaren Satz beschreiben lässt, fehlt häufig nicht nur sprachliche Präzision, es fehlt in Wahrheit ein Teil des Projekts selbst. Denn unklare Ziele führen fast immer zu unklaren Grenzen. Und wo Grenzen unklar bleiben, werden Verantwortlichkeiten, Rechtsgrundlagen und Schutzmaßnahmen ebenfalls unscharf.

Zur Entscheidungsklarheit gehört deshalb mehr als ein abstraktes Zielbild. Es braucht einen greifbaren Scope. Welche Daten sind betroffen? Welche Personengruppen? Welche Systeme und welche Schnittstellen? Wer ist fachlich verantwortlich und wer operativ zuständig? Diese Fragen klingen banal. In der Projektrealität sind sie es selten. Gerade der Punkt der Zuständigkeit führt in Besprechungen regelmäßig

zu jener stillen Sekunde, in der plötzlich für die Meetingteilnehmer jede Kaffeetasse interessanter wirkt als die eigene Verantwortung.

Datenschutzbeauftragte können hier einen erheblichen Mehrwert liefern. Indem sie Entscheidungen entscheidungsfest machen und eben nicht, indem sie den Prozess bremsen. Empfehlenswert ist dafür eine schlanke Entscheidungsvorlage für Innovationsprojekte – bewusst knapp, möglichst auf einer Seite. Darin enthalten sein sollten das Zielbild, die betroffenen Daten und Personengruppen, die Rollen und Verantwortlichkeiten sowie die Nachweise, also etwa Verweise auf das Verzeichnis von Verarbeitungstätigkeiten, technische und organisatorische Maßnahmen, DSFA-Prüfung, Verträge und Freigaben. Das ist keine Bürokratie, das ist ein „Wir machen mal“-Vorhaben, das eine Organisation verantworten kann. Entscheidungsklarheit schafft damit die erste Vertrauensbasis für alle Beteiligten. Sie gibt Projekten Richtung. Sie zwingt dazu, Zweck und Grenzen zu benennen. Und sie stellt sicher, dass Verantwortung nicht als kollektive Nebelzone organisiert wird, sondern als konkrete Zuständigkeit.

2. Risikoklarheit: Nicht Angst, sondern Frühwarnsystem

Der zweite Baustein tragfähiger Innovation ist Risikoklarheit. Auch hier lohnt ein Perspektivwechsel. Risikoklarheit bedeutet nicht Alarmismus. Sie bedeutet nicht, sich von Haftungs- oder Aufsichtsszenarien lähmen zu lassen. Und sie bedeutet schon gar nicht, jedes Projekt mit maximalem Prüfaufwand zu überziehen. Risikoklarheit heißt vielmehr: Wir wissen, wo es knirschen kann – und wir merken es früh.

Gerade Innovationsvorhaben verändern Prozesse, Datenflüsse, Berechtigungen und Abhängigkeiten. Risiken entstehen deshalb nicht erst, wenn etwas schief läuft. Sie entstehen bereits dort, wo Organisationen die Folgen ihrer Entscheidungen nicht vollständig sehen. In der Praxis zeigen sich dabei immer wieder ähnliche Muster.

Ein erstes Muster lautet: „Das ist doch nur ein Tool.“ Wer das sagt, unterschätzt regelmäßig die Tragweite technischer Einführungen. Tools sind nie nur Tools. Sie verändern Zugriffe, erzeugen Schnittstellen, schaffen neue Dienstleistungsrollen, neue Exportmöglichkeiten und mitunter auch neue Schatten-IT. Die eigentliche Frage lautet daher nicht, ob ein Tool eingesetzt wird. Die eigentliche Frage ist, welche Entscheidung bereitet es vor oder trifft es – und wer diese Entscheidung prüft. Denn wenn niemand prüft, ist das einfach nur Hoffungsmanagement.

Ein zweites Muster ist der Verweis auf später: „Wir pseudonymisieren oder anonymisieren später.“ „Später“ ist in vielen Organisationen ein bemerkenswert belastbares Da-

tum. Es liegt irgendwo zwischen nächster Woche und nie. Gerade bei Datenminimierung ist diese Logik gefährlich. Denn was nicht erhoben wird, muss später weder geschützt noch erklärt noch bereinigt werden. Die entscheidende Frage lautet daher: Welche Daten sind wirklich erforderlich – und welche sind lediglich bequem? Bequemlichkeit ist aus datenschutzrechtlicher Sicht selten ein tragfähiges Sicherheitskonzept. Es ist ein weiteres Risiko.

Ein drittes Muster ist die trügerische Sicherheit: „Wir haben ja ein Banner.“, „Wir haben eine Einwilligung.“, „Wir haben ein Häkchen.“ Wenn Vertrauen ein Häkchen wäre, wären wir alle schon vor Jahren fertig gewesen. Und das Internet wäre insgesamt ein ruhigerer Ort. Im Einzelfall kann das richtig und erforderlich sein. Es ersetzt aber keine tragfähige Prüfung der tatsächlichen Rechtsgrundlage, des Zwecks und der Erwartungshaltung der Betroffenen. Vertrauen entsteht nicht aus Kästchen zum Anklicken. Vertrauen entsteht aus einer Verarbeitung, die inhaltlich passt und erklärt werden kann. Auch die Rechtsgrundlage ist deshalb nicht nur Juristerei. Sie ist immer auch Kommunikations- und Erwartungsmanagement.

Für Risikoklarheit braucht es keinen reflexhaften Hang zu 80 Seiten Papier. Was Organisationen brauchen, ist ein robuster, wiederholbarer Ablauf. Ein strukturierter Kurz-Risiko-Check zu Beginn eines Projekts kann bereits genügen, um die wesentlichen Punkte sichtbar zu machen. Danach folgt die Entscheidung: Handelt es sich um einen Standardprozess oder ist eine vertiefte Prüfung, etwa eine DSFA, erforderlich? Anschließend müssen Maßnahmen, Verantwortlichkeiten und Nachweise nachvollziehbar dokumentiert werden. Dahinter steht ein ebenso einfacher wie wirksamer Grundsatz: Risiken an sich sind nicht das Problem, unsichtbare, nicht erkannte Risiken sind es.

3. Kommunikationsklarheit: Vertrauen entsteht, wenn Menschen verstehen, was passiert

Der dritte Punkt wird in der Praxis besonders häufig unterschätzt: Kommunikationsklarheit. Viele Organisationen investieren erhebliche Zeit in technische Prüfungen, Prozesse, Vertragswerke und Dokumentation. Das ist richtig und notwendig. Doch selbst ein fachlich sauber aufgesetztes Projekt kann an Akzeptanz verlieren, wenn am Ende niemand mehr verständlich erklären kann, was mit den Daten passiert und warum.

Kommunikationsklarheit beantwortet im Kern drei Fragen: Was passiert mit den Daten? Warum passiert das? Und was bedeutet das für die Betroffenen – einschließlich der Frage, welche Einfluss- und Kontrollmöglichkeiten sie haben. Diese Fragen wirken einfach. Und gerade deshalb sind sie anspruchsvoll. Denn sie verlangen eine Sprache, die juristisch

korrekt bleibt, ohne sich im Juristendeutsch zu verlieren; die technisch präzise ist, ohne nur für Spezialisten verständlich zu sein; und die organisatorisch anschlussfähig bleibt, ohne den Kern zu verwässern.

Hier liegt eine der wichtigsten Rollen professioneller Datenschutzarbeit. Datenschutzbeauftragte sind Übersetzerinnen und Übersetzer. Sie vermitteln zwischen Juristendeutsch und Alltagssprache, zwischen IT-Realität und Management-Entscheidung, zwischen Aufsichtsperspektive und Organisationspraxis, zwischen normativer Anforderung und alltagstauglicher Umsetzung. Kommunikationsklarheit bedeutet daher nicht, Komplexität zu verleugnen. Sie bedeutet, klar zu sagen, was Sache ist – ohne ‚Nebelmaschine‘.

Für Innovationsprojekte ist das von zentraler Bedeutung. Wer Innovation ernst meint, muss Erklärbarkeit ernst nehmen. Denn fehlende Verständlichkeit erzeugt Misstrauen selbst dann, wenn im Hintergrund vieles richtig läuft. Umgekehrt kann eine gute, klare Erklärung dazu beitragen, dass notwendige Maßnahmen nachvollzogen und akzeptiert werden – intern wie extern. Gerade in sensiblen Verarbeitungskontexten wird damit aus Kommunikation ein Element der Risikosteuerung.

Datenschutz als Brücke zwischen Aufsicht und Organisation

Die besondere Relevanz dieser drei Klarheiten zeigt sich dort, wo unterschiedliche Perspektiven zusammenkommen. Aufsichtsbehörden bringen Orientierung und Maßstäbe ein. Das ist unverzichtbar, gerade in Zeiten, in denen technologische Entwicklungen schneller voranschreiten als viele etablierte Governance-Strukturen. Organisationen wiederum bringen die operative Realität ein: Zeitdruck, knappe Ressourcen, Transformationsaufgaben, Erwartungsdruck von innen und außen.

Datenschutzbeauftragte sitzen häufig genau zwischen diesen Polen. Und genau darin liegt ihre eigentliche Stärke. Sie übersetzen nicht nur rechtliche Anforderungen in organisatorische Praxis. Sie sorgen zugleich dafür, dass operative Machbarkeit nicht auf Kosten von Nachvollziehbarkeit, Schutz und Verantwortbarkeit geht. Aufsicht braucht Nachvollziehbarkeit. Organisationen brauchen Machbarkeit. Vertrauen braucht beides.

Der Dreiklang aus Entscheidungsklarheit, Risikoklarheit und Kommunikationsklarheit eignet sich deshalb als gemeinsamer Nenner für diese unterschiedlichen Erwartungen. Er macht Datenschutz anschlussfähig, ohne ihn zu entkerneu. Er stärkt die Handlungsfähigkeit von Verantwortlichen, ohne Risiken auszublenden. Und er unterstützt eine Praxis, in der Datenschutz weder Gegenspieler der Innova-

tion noch bloßer Dokumentationsanhang ist, sondern gemeinsame Sprache.

FAZIT

Zweck. Risiko. Erklärung.

Innovation braucht heute mehr als Technikbegeisterung und gute Absichten. Sie braucht einen klaren Zweck, damit aus Innovation keine Spielerei wird. Sie braucht ein funktionierendes Frühwarnsystem, damit aus einem Pilotprojekt kein Vorfall wird. Und sie braucht verständliche Sprache, damit nicht alles formal richtig ist, aber niemand überzeugt wird. Diese drei Elemente sind keine Nebensächlichkeiten. Sie sind die Voraussetzungen dafür, dass Innovation im Alltag tragfähig bleibt.

Datenschutz ist in diesem Verständnis kein nachgelagerter Prüfstein. Er ist integraler Bestandteil guter Organisationsentscheidungen. Er macht Projekte nicht kleiner, sondern belastbarer. Nicht langsamer, sondern tragfähiger. Nicht weniger innovativ, sondern anschlussfähig. Wer Innovation verantwortungsvoll gestalten will, sollte Datenschutz deshalb nicht erst dann hinzuziehen, wenn es ungemütlich wird, sondern bereits dann, wenn die Richtung festgelegt werden soll.

Oder, kalenderfähig: Zweck. Risiko. Erklärung.

Das ist der Sicherheitsgurt.

Grundlage dieses Beitrags ist die von der Autorin im Rahmen des 2. Mitteldeutschen Datenschutztages am 10. März 2026 in Erfurt gehaltene Begrüßungs-Keynote „Innovation mit Sicherheitsgurt: Vertrauen entsteht durch gute Entscheidungen – nicht durch gute Absichten“.

Über die Autorin

Regina Mühlich

ist Wirtschaftsjuristin, externe Datenschutzbeauftragte und Compliance Manager, Vorständin des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V. und Beirätin der Stiftung Datenschutz. In ihrer Beratungspraxis beschäftigt sie sich insbesondere mit der praxistauglichen Umsetzung datenschutzrechtlicher Anforderungen an der Schnittstelle von Organisation, Digitalisierung und Governance.



BvD-Kongresse
2027

Save the Date

**Jetzt Termine
vormerken**

3. Mitteldeutscher Datenschutztag

17.03.2027 in Dresden

BvD-Verbandstage 2027

11.-12.05.2027 in Berlin



Jetzt anmelden

bvdnet.de/de/veranstaltungen/konferenzen/

