

---

## Alles anders? Gängige Irrtümer zum neuen Datenschutz

---

**So groß die Aufregung war, als am 25. Mai 2018 die DSGVO geltendes Recht wurde, so wenig schien sich zunächst zu ändern. Viele Begriffe kamen den Beteiligten vertraut vor. Bei näherer Betrachtung sieht Datenschutz heute allerdings in vielen Bereichen grundlegend anders aus als nach früherem Recht. Mit dem bisherigen Verständnis gehen mitunter folgenreiche Missverständnisse einher, die bis heute weit verbreitet sind. Erst nach und nach dämmert es Datenschützern, dass das neue Datenschutzrecht europäisch ist – und damit deutlich zeitgemäßer, als es das alte jemals war.**

**Neues Recht:** Am 25. Mai 2016 trat die Datenschutz-Grundverordnung in Kraft und war zwei Jahre später rechtsverbindlich. Damals waren die meisten aus der kleinen Gruppe derer, die mit dem „alten“ Datenschutz einigermaßen vertraut waren, der Meinung, dass sich mit dem neuen (europäischen) Recht eigentlich nicht allzu viel geändert habe.

**Situation:** Jetzt, da einige Zeit vergangen ist, wird manchem bewusst, wie gravierend anders die Rechtslage tatsächlich ist – und wie zahlreich die Irrtümer im Umgang damit. Gerade hierzulande scheint sich erst nach und nach herumzusprechen, wohin sich der Datenschutz derzeit entwickelt. Viele Chancen bleiben ungenutzt.

**Neue Chancen:** Es mag sich also lohnen, genauer hinzusehen: Was ist anders mit der neuen Rechtslage? Was unterscheidet europäisches Recht vom deutschen? Welches sind seit der DSGVO die größten Irrtümer – und wie lassen sich die Möglichkeiten nutzen, die das neue Datenschutzrecht mit sich bringt?

**Risikomanagement:** Faktisch ist Datenschutz heute Teil des Risikomanagements, sein Ansatz an vielen Stellen risikoorientiert. Wie und in welchem Umfang Daten zu schützen sind, bemisst sich daran, welche Risiken für die Rechte und Freiheiten der Betroffenen bestehen.

**Rechtslage:** Bei der DSGVO handelt es sich um europäisches Recht. Genauer gesagt: um eine europäische Grundverordnung. Damit ist sie unmittelbar rechtsverbindlich für alle EU-Mitgliedsstaaten. Verhandlungssprache war Englisch, Grundlage ist Recht nach angelsächsischer Auslegung. Dank zahlreicher Öffnungsklauseln können die EU-Staaten in

nationalen Gesetzen Verschärfungen festlegen. So weit, so bekannt.

**Folgen nicht immer bekannt:** Welche Folgen diese Fakten aber im Einzelnen nach sich ziehen, gerade im Bereich Datenschutz, darüber sind sich nur wenige im Klaren. Wem europäische Rechtsauslegung neu ist, kann grundlegende Begriffe und Prinzipien schnell missverstehen. Einige solcher Irrtümer begegnen uns Datenschützern im Alltag leider immer wieder. Sie haben Folgen – Datenschutz wird falsch umgesetzt oder verursacht Aufwand, der sich vermeiden ließe.

**Irrtum Nr. 1: Alles mit Einwilligung** Die Folgen eines dieser Missverständnisse dürfte jeder von uns am Inhalt seines E-Mail-Postfachs zu spüren bekommen haben, als das neue Recht bindend wurde. Nehmen wir den Kunden eines Onlineshops, den nach seiner Bestellung eine E-Mail des Lieferanten erreicht. Man sei verpflichtet, heißt es darin, die Daten aus der Bestellung für eine mögliche Betriebsprüfung durch die Finanzverwaltung zehn Jahre lang aufzubewahren. Laut DSGVO sei hierzu die Einwilligung des Kunden erforderlich, er solle diese bitte erteilen und zurücksenden.

**Recht auf Widerspruch?** All jenen, die nun nicht tadelnd den Kopf schütteln: Für Verarbeitungen, die auf einer rechtlichen Verpflichtung fußen, benötigen Verantwortliche natürlich keine Einwilligung des Betroffenen. Sie „zusätzlich“ oder „zur Sicherheit“ einzuholen, sollten sie auch tunlichst vermeiden. Nicht jede Aufsichtsbehörde begrüßt es, wenn Verantwortliche mit der Einwilligung ein Recht auf Widerspruch vorzugaukeln, das in Wahrheit nicht besteht.

**Irrtum Nr. 2: Grundrechte** Die Europäische Grundrechtecharta (GRCh) hat als verbindlicher Überbau über das Datenschutzrecht das deutsche Grundgesetz abgelöst. Ein Umstand, der begrifflicherweise Verwirrung nach sich zieht.

**Videoüberwachung und Grundrechte:** Ein Beispiel? Die datenschutzrechtliche Behandlung der Videoüberwachung. Man lese hierzu Art. 6 GRCh im Vergleich zu Art. 2 des Grundgesetzes. Schnell wird klar, warum andere EU-Länder mit Videoüberwachung kaum ein Problem haben. Ein „Recht auf freie Entfaltung der Persönlichkeit“ im deutschen Grundgesetz besitzt andere Schwerpunkte als das „Recht auf Freiheit und Sicherheit“ der europäischen Grundrechtecharta.

**Neue Rechtslage:** Es ist empfehlenswert, sich die Chancen der geänderten Rechtslage vor Augen zu führen (man beachte das Urteil vom 27.03.2019 BVerwG 6 C 2.18, wo § 4 Abs. 1 Satz 1 BDSG n. F. in Teilen als nicht mit europäischem Recht konform entlarvt wird). Mancher mag enttäuscht festgestellt haben, dass die Videoüberwachung in der DSGVO keine Erwähnung findet. Das jedoch heißt nichts anderes, als dass sich ihre Rechtmäßigkeit an deren allgemeinen Maßstäben bemisst. Damit ist Videoüberwachung grundsätzlich möglich, aber es müssen eben gewisse Voraussetzungen erfüllt sein. Etwa, dass die verfolgten Ziele nicht mit milderem Mitteln erreicht werden können und angemessene Schutzmaßnahmen getroffen werden. Verantwortlichen bleibt Freiraum – solange sie Abläufe begründen und verantwortungsvoll gestalten.

**Irrtum Nr. 3: Aufgaben der Aufsichtsbehörden** Beratung war früher. Einstmals hatte eine deutsche Aufsichtsbehörde neben anderen Aufgaben auch die der Beratung inne: „Sie berät und unterstützt die Beauftragten für den Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse“ – so stand es früher im BDSG.

**Aufsichtsbehörde berät nicht mehr:** Demgegenüber haben Aufsichtsbehörden laut neuem Recht eine ganze Liste von Aufgaben, 22 an der Zahl. Keine davon fordert die Beratung der Verantwortlichen. Einzige Ausnahme: die Beratung nach einer Meldung bei einer Datenschutz-Folgenabschätzung, bei der ein hohes Risiko die Folge sein könnte. Sind Klagen, die Aufsichtsbehörden würden bei Anfragen von Verantwortlichen keine verbindlichen Aussagen treffen, überhaupt gerechtfertigt?

**Sensibilisierung statt Beratung:** Was heute zu den Aufgaben der Datenschutz-Aufsichtsbehörden zählt, ist die Sensibilisierung unter anderem der Verantwortlichen. In Deutschland hat das die Datenschutzkonferenz in Abstimmung mit dem Europäischen Datenschutzausschuss in aktuell 20 Kurzpapieren zu den wichtigsten Datenschutzthemen umgesetzt. Sie sind die einzigen halbwegs verbindlichen Aussagen der Aufsichtsbehörden zu den aktuellen Umsetzungsfragen im Datenschutzrecht, die es derzeit gibt.

**Verantwortlich bedeutet Verantwortung:** Es mag bequem erscheinen, wenn die Aufsichtsbehörden verbindliche Auskünfte erteilen würden. Doch Verantwortliche tragen die Verantwortung. Schließlich wurde dafür der Ansatz der Risikoorientierung in die DSGVO aufgenommen. Welche Chance, wenn man sie nutzen möchte!

**70x Risiko in der DSGVO:** Nicht umsonst hat der Gesetzgeber in die DSGVO und die Erwägungsgründe rund 70 Mal den Begriff des Risikos in mehreren Formen und Anwendungen aufgenommen. Datenschutz als Risikomanagement? Für manchen mag dieser Ansatz verwundernd sein. Für Unternehmen, die in der Digitalisierung angekommen sind, ist er der einzige Weg, die Anforderungen adäquat umzusetzen.

**Irrtum Nr. 4: Alles verboten** Nach früherem Datenschutzrecht herrschte Einigkeit. Das alte BDSG war ein „Verbotsgesetz mit Erlaubnisvorbehalt“. Datenverarbeitung war danach nur zulässig, soweit das BDSG selbst oder eine andere Rechtsvorschrift sie erlaubten oder anordneten – oder mit Einwilligung des Betroffenen. Zahlreiche Kommentatoren und Redner sprechen aber bis heute davon, die DSGVO sei ein „Verbotsgesetz mit Erlaubnisvorbehalt“. Stimmt das nicht?

**Verbotsgesetz?** Sieht man sich Artikel 1 der DSGVO näher an, so wird darin ein Verbot verboten. Denn: „Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.“ Ruft man sich den risikoorientierten Ansatz der Verordnung in Erinnerung, handelt es sich bei der Umsetzung des Datenschutzes heute eher um die Bewältigung von Risiken, die bei der Verarbeitung personenbezogener Daten entstehen. Prozesse sind zu erfassen, zu prüfen und zu gestalten. Über vermeintlich geltende Verbote zu sprechen, hilft nicht weiter.

**Raum für Gestaltung:** Die Anforderung des Art. 6 DSGVO, dass eine Verarbeitung eine Rechtsgrundlage benötigt, ist ein ganz normaler Vorgang. Natürlich muss eine Verarbeitung rechtmäßig sein. Allerdings sind die sechs potenziellen Rechtsgrundlagen, aus denen man nach EU-Recht die zutreffende wählen kann, so vielfältig, dass man hier nicht von einem Verbotsgesetz sprechen sollte. Viel treffender kann man sagen: Die DSGVO ist ein Gestaltungsgesetz.

**Datenschutz gestalten:** Warum das wichtig ist? Da ein „Verbotsgesetz“ auf Beschäftigte mitunter äußerst erschreckend wirkt. Verarbeitung personenbezogener Daten wird damit etwas Gefährliches, das man besser nicht riskiert. Das allerdings wird dem Charakter der DSGVO nicht gerecht. Es ist nicht der Wille des Gesetzgebers, Prozesse zu verbieten, sondern Abläufe datenschutzgerecht gestaltet zu wissen. Artikel 1 macht es deutlich.

**DSGVO als Chance:** Angesichts der Herausforderungen der Digitalisierung hilft Gerede vom „Verbotsgesetz“ nach vermeintlich gutem altem Recht nicht weiter. Weit ratsamer ist es, die Möglichkeiten der DSGVO zu erkennen

und zu nutzen. Das Datenschutzrecht ist zeitgemäß geworden – eine wunderbare Chance für alle, die es umsetzen!

**Ausblick:** Es zeigt sich: Datenschutz ist heute nicht nur deutlich moderner, er bietet auch Raum für Lösungen und gestalterische Freiheit. Und genau das macht ihn spannend! Wer mehr wissen möchte über modernen Datenschutz – Themen wie Auftragsverarbeitung, technische und organisatorische Maßnahmen und Beschäftigtendatenschutz folgen in den kommenden Praxistipps.

### **Rechtsquellen zum Nachlesen**

Zur **Datenschutz-Folgenabschätzung:** Art. 35 Abs. 3 lit. c DSGVO

Zu den **Aufgaben der Aufsichtsbehörden:** Art. 57 Abs. 1 DSGVO, § 38 Abs. 1 Satz 2 BDSG a. F.

Zum **Verbotsgesetz:** § 4 Abs. 1 BDSG a. F., Art. 1 Abs. 3 DSGVO

**Alle Praxistipps gibt es auf [team-datenschutz.de](https://www.team-datenschutz.de)**

**Hier schreibt Eberhard Häcker, Externer Datenschutzbeauftragter, Datenschutzberater, Fachautor und Kongressredner, Geschäftsführer der TDSSG GmbH – Team Datenschutz Services – und der HäckerSoft GmbH (Datenschutz-Software DATSIS und Lernplattform Optilearn.de). Er ist überzeugt, „den spannendsten Beruf der Welt“ zu haben, denn Datenschutz unter der DSGVO ist „wie die Besiedlung Amerikas – weißes Land, das es zu entdecken und sinnvoll zu füllen gilt“. (Eberhard Häcker)**