Ausgabe 02/2021

ISSN: 2194-1025

# BvD-NEWS

Das Fachmagazin für den Datenschutz

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

## DIGITALISIERUNG UND DATENSCHUTZ SO GELINGT DIE TRANSFORMATION



BvD e.V.
DATENSCHUTZ GESTALTEN

# EDITORIAL

## Liebe Leserinnen und Leser,

als im vergangenen Frühjahr der erste Corona-Lockdown begann, hätte wohl keiner vermutet, dass die Überwindung des Virus auch über ein Jahr später noch das Thema sein wird, das die Politik, die Medien und unser aller Leben tagtäglich bestimmt. Auch um gegen den Datenschutz ins Feld zu ziehen, wird die Pandemie mittlerweile schamlos von den üblichen Lagern instrumentalisiert: Datenschutz sei angeblich ein Innovationshemmnis im Kampf gegen Corona. Einige sprechen sogar davon, dass Datenschutz Menschen töte. Das Erschreckende an diesen absurden Botschaften: Oft werden sie unhinterfragt von den Medien weitergetragen.

Die Mär vom Datenschutz als Innovationshemmnis ist natürlich nicht neu. Auch in den Diskursen um die Digitalisierung Europas wird man nicht müde sie zu wiederholen. Ebenso hartnäckig wiederholen wir als BvD daher, dass man sowohl in der Pandemie als auch beim Thema Digitalisierung den Datenschutz nicht als Sündenbock missbrauchen darf, um die eigentlichen Probleme zu verschleiern. Bei Ersterer sind dies neben der schlechten Pandemie-Prävention selbst eher unsere schlecht ausgestattete Verwaltung und die mangelnde Abstimmung von Plänen über Länder- und Kommunengrenzen hinweg. Bei Letzterer sollte das Augenmerk darauf gerichtet sein, Europas digitale Souveränität durch gezielte Förderung von europäischen Lösungen für die Zukunft zu sichern.

Dass wir mit dieser Auffassung nicht alleine sind, zeigte sich bei unseren erneut digital abgehaltenen BvD-Verbandstagen (Nachbericht ab Seite 5), bei denen beispielsweise BfDI Prof. Ulrich Kelber und BlnLDI Maja Smoltczyk auf diese irreführende Argumentation hinweisen. Nachzulesen ist dies auch im vorliegenden Heft, denn– wie es mittlerweile schöne Tradition ist – konnten wir erneut ausgewählte Referentinnen und Referenten des Kongresses dafür gewinnen, Gastbeiträge zu verfassen.

Wenn es nun also darum geht, Digitalisierung und Datenschutz zusammenzudenken, „kommt den Datenschutzbeauftragten in Unternehmen und Verwaltungen eine Schlüsselrolle zu“, betont Ulrich Kelber. Wir werden zu Wegbegleitern, zu „Lotsen“ bei der Entwicklung und der Einführung neuer digitaler Technologien – wie es auch das Motto unserer Verbandstage treffend formulierte. Dieses Rollenverständnis des DSB zu vermitteln, ist vornehmste Aufgabe des BvD, sowohl bei Verantwortlichen als auch bei uns Datenschutzbeauftragten selbst.

Wenn sich diese Perspektive durchsetzt und folgerichtig auch die Notwendigkeit verstanden wird, Datenschutzbeauftragte frühzeitig in Digitalisierungsprojekte einzubinden, dann wird Datenschutz endlich nicht mehr als Innovationshemmniss missverstanden und der Datenschutzbeauftragte nicht mehr als Bedenkenträger, sondern als Ermöglicher. Als Ermöglicher von Innovationen, die rechtssicher für die Verantwortlichen sind und das Vertrauen der Nutzer genießen. So sollte „Digitalisierung made in Europe“ aussehen. Lassen Sie es uns gemeinsam angehen!

Ich wünsche Ihnen eine anregende Lektüre.

Thomas Spaeing
BvD-Vorstandsvorsitzender

**IMPRESSUM:**

BvD-News

Das Fachmagazin des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e.V.

**Herausgeber:**

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.
Budapester Straße 31
10787 Berlin
Tel: 030 26 36 77 60
Fax: 030 26 36 77 63
E-Mail: bvd-gs@bvdnet.de
Internet: www.bvdnet.de
www.xing.com/companies/berufsverbandderdatenschutzbeauftragtendeutschlands
www.twitter.com/bvd_datenschutz
www.bvdnet.de/feed/

**Redaktion:**

Christina Denz (chd)
V.i.S.d.P.: Thomas Spaeing
bvd-news@bvdnet.de

**Fotos (sofern nicht anderweitig ausgewiesen):**

www.123rf.com

**Lektorat:**

Frank Spaeing, Regina Mühlich

**Anzeigen:**

Christina Denz
Kooperationen: Karsten Füllhaase (bvd-gs@bvdnet.de)

**Satz, Layout & Produktion:**

Trend Point Marketing GmbH,
Breitenbachstraße 24-29, 13509 Berlin
www.tpmarketing.de

ISSN: 2194-1025

Erscheinungsweise: 3 x jährlich, Druckauflage 4.000 Exemplare (Unsere Mediadaten erhalten Sie unter bvdnet.de/Publikationen oder von unserer Geschäftsstelle per E-Mail an bvd-gs@bvdnet.de) Die Redaktion behält sich vor, Beiträge redaktionell zu überarbeiten und zu kürzen. Namentlich gekennzeichnete Beiträge müssen nicht die Meinung des BvD e.V. wiedergeben

# FAIR PLAY BEI DER DIGITALISIERUNG

## Auf den BvD-Verbandstagen wehren sich DSB und Aufsichtsbehörden gegen Vorwürfe, Datenschutz behindere die Digitalisierung

Jürgen Hartz


BvD-Vorstandsmitglied Kai-Uwe Loser im Gespräch mit der Landesbeauftragten für Datenschutz Schleswig-Holstein, Marit Hansen. Sie sprach darüber, wie Datenschutzbeauftragten die Arbeit schwergemacht wird.

Sportler lieben Fair Play, aber warum tun sich Unternehmen und Behörden so schwer mit Fair Play in der Digitalisierung? Datenschutz ist zum Sündenbock geworden, das betonte nicht nur Christian Spancken, Unternehmensberater und nach eigenen Angaben nicht verdächtig, dem Datenschutz generell eine Lanze zu brechen. Aber als Unternehmensberater und Speaker sieht er selbst: Wir kaufen lieber bei einem Unternehmen, dem wir vertrauen können.

Spancken hielt die Keynote zum Auftakt der zweiten rein virtuellen BvD-Verbandstage vom 19. bis 21. Mai 2021. Und nicht nur er stellte fest: Datenschutz ist zum Sündenbock geworden, vor allem in der Hauruck-Digitalisierung während der Corona-Pandemie. Datenschutz muss als Grund herhalten, wenn die Digitalisierung im Gesundheitsbereich nicht vorankommt, wenn Unternehmen sich und ihre Angestellten nicht rechtzeitig auf mobiles Arbeiten und aufs Homeoffice vorbereitet haben, wenn Schulen sich vor der Pandemie offenbar wenige Gedanken um digitale Anwendungen gemacht haben und wenn manche Verwaltung noch lieber mit Faxgerät arbeitet statt mit E-Mail. Ihnen allen ist das pandemiebedingte Digitalisierungstempo auf die Füße gefallen und zeigt deutlich Versäumnisse der Vergangenheit auf.

Aber wer sich vorher nicht oder nur unzulänglich Gedanken um die Digitalisierung gemacht hat, dem muss Datenschutz, vor allem die Datenschutz-Grundverordnung (DSGVO) wie ein Buch mit sieben Siegeln vorkommen. Das hat aber nichts mit dem Datenschutz zu tun, sondern mit dem niedrigen Digitalisierungs-Niveau in


BvD-Vorstandsvorsitzender Thomas Spaeing im Gespräch mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Ulrich Kelber.

vielen Unternehmen und insbesondere in Behörden. Dabei ist die Digitalisierung nicht eine Erfindung der Pandemie. Seit drei Jahren gilt die DSGVO, aber manche fühlen sich vom Datenschutz immer noch überrascht. Wie viele jammerten, durch den „bösen Datenschutz" gehe die Volksgesundheit den Bach herunter, schreibt Bundesdatenschutzbeauftragter Ulrich Kelber in seinem Beitrag. Da werde „immer mehr mit dem Bauchgefühl hantiert" anstatt sich die Fakten und Sachlage genau anzuschauen. Immer wieder wurde behauptet, wie Ulrich Kelber ausführt, dass der Datenschutz das einzige Grundrecht sei, dass in der Pandemie unangetastet geblieben wäre. „Das ist natürlich vollständiger Unsinn", schreibt er. Aber es zeigt, wie Stimmung gegen Datenschutz und mitunter auch gegen uns Datenschutzbeauftragte gemacht wird.

## Verantwortung des Staates

„Datenschutz heißt nicht Datenaskese", stellte Dirk Heckmann klar, Rechtsprofessor am Lehrstuhl für Recht und Sicherheit der Digitalisierung an der TU München. Der renommierte Internet-Rechtsexperte und nebenamtliche Verfassungsrichter am Bayerischen Verfassungsgericht fand es richtig in der Pandemie auch den Datenschutz wie andere Freiheitsrechte zum Schutz der Bevölkerung einzugrenzen. Aber die Verwaltungen müssten diese Daten nutzen, um die Gefahrenvorsorge vor weiteren Pandemie-Ausbrüchen zu verbessern.

Da zeige sich, dass die Daten nicht wegen des Datenschutzes ungenutzt blieben, sondern wegen der Überalterung der Verwaltungsstrukturen. „Ein Staat, der grundrechtsschützende Digitalisierung ignoriert, verletzt seine Schutzpflicht und handelt ethisch unverantwortlich", argumentierte Heckmann. „Wir werden noch diskutieren müssen über die Verantwortung des Staates", sagte er.

## Datenschutz ist „kein Sahnehäubchen"

Für die Berliner Beauftragte für Datenschutz und Informationsfreiheit Maja Smoltczyk, neben der Brandenburgischen und der niedersächsischen

Aufsichtsbehörde Partner der diesjährigen Verbandstage, ist Datenschutz „kein Sahnehäubchen". Datenschutz gehört für sie an den Anfang von Projekten, von Prozessen und Produktentwicklungen. Er müsse Teil des Leistungspakets sein, das Verwaltungen ausschreiben, um neue Projekte oder Aufträge zu vergeben, verlangte sie. Nur wenn die Verwaltung Datenschutz garantiere, fassten die Bürgerinnen und Bürger Vertrauen in den Staat, argumentiert sie in ihrem Beitrag in dieser Ausgabe.

Dabei sei Datenschutz ein Grundrecht und nicht - wie in der Pandemie häufig argumentiert - ein zentrales Problem der Digitalisierung. Viele Menschen machten sich sehr wohl Gedanken über ihre persönlichen Daten. Es sei weder unangemessen noch unrealistisch, jetzt, mit dem Abflauen der Pandemie, die Umstellung auf datenschutzrechtliche Produkte und Verfahren zu fordern. Die Pandemie zeige „wie durch ein Brennglas" auf die Baustellen der Digitalisierung.

## Wirksamer Datenschutz weckt Kundenvertrauen

Anders als in vielen Verwaltungen haben manche Unternehmen Datenschutz als Schlüssel für Kundenvertrauen erkannt, etwa bei der REWE Group. Katrin Tresp leitet deren zentrales Datenschutzmanagement und gab in ihrem Vortrag Einblick in die Bedeutung von Kundendaten und deren Sicherheit für den Lebensmittelkonzern. REWE entwickelte danach eine eigene Corporate Digital Responsibility (CDR), die über die gesetzlichen Regelungen hinausgeht. Tresp versteht die Guidelines als Unterstützung der Digitalisierung. Solche Selbstverpflichtungen förderten die digitale Kompetenz von Unternehmen und könnten insbesondere für Social Entrepreneure Kunden-Vertrauen aufbauen. Nur mit einer CDR ist aus ihrer Sicht die Öffnung für den Datenverkehr möglich – unter Einhaltung der Gesetze und einer gemeinsamen Datenethik.

Tresp ist überzeugt, dass der Bedarf an fachlicher Beratung zum Datenschutz in den nächsten Jahren noch zunehmen wird, und zwar bei Unternehmen wie auch bei behördlichen Stellen. „Es wird eine Herausforderung sein, die Diskussion um die Ressourcen zu führen", sagte Tresp.

## Role Model DSGVO

Dabei ist Europa mit der DSGVO gut aufgestellt, befand Renate Nikolay, Kabinettchefin von EU-Vizepräsidentin Věra Jourová. Sie gab Einblick in den „Brüsseler Maschinenraum", wo derzeit die Grundlagen für ein neues EU-US Privacy Shield und neue Standardvertragsklauseln vorbereitet werden,


Die Vorsitzenden der nationalen Datenschutzbeauftragten-Verbände aus Österreich, der Schweiz, Tschechien, Liechtenstein und Frankreich im Gespräch mit BvD-Vorsitzendem Thomas Spaeing.

allerdings „nicht so schnell, damit wäre keinem gedient“, sagte Nicolay in ihrem Vortrag. Dass aber in Europa mit dem Start der DSGVO vor fast genau drei Jahren ein neues digitales Selbstbewusstsein erwachte, daran ließ sie keinen Zweifel. Nicolay berichtete von den Verhandlungen mit Japan und Korea über eigene Datenschutz-Bestimmungen. Der Weg in die Zukunft könne nicht protektionistisch wie in China gedacht werden, sondern liege in einem offenen Austausch, in dem Europa klar seine Bedingungen und Werte benennen muss.

## Happy Birthday DSGVO

Wie es um den Datenschutz in Zeiten der Pandemie in anderen europäischen Ländern aussieht, erläuterten Kolleginnen und Kollegen aus Frankreich, Liechtenstein, der Schweiz, Österreich und Tschechien in der Diskussionsrunde-Runde des vom BvD mitgegründeten Dachverbands EFDPO anlässlich des dritten Geburtstags der DSGVO.


Snack-Pack des BvD für die Teilnehmenden an den BvD-Jahrestagen 2021

In Österreich macht Judith Leschanz, Vorstandsvorsitzende des Vereins österreichischer betrieblicher und behördlicher Datenschutzbeauftragter – Privacyofficers.at, noch ein Defizit vor allem bei kleinen und mittelständischen Betrieben bei der Umsetzung der DSGVO aus. Allerdings werde Datenschutz durchaus als Kundenvorteil verstanden, weil auch die „Awareness“ der Bürgerinnen und Bürger im Heimatland von Datenschutzaktivist Max Schrems beim Thema Datenschutz hoch sei. Der Kunde wolle Datenschutz „als Grundrecht, das ihm gebührt“.

In der Schweiz wird das neue nationale Datenschutzgesetzt voraussichtlich 2022 in Kraft treten, wie Jérôme Egli, Präsident der Data Privacy Community, sagte. Viele der internationalen in der Schweiz ansässigen Unternehmen hätten sich schon aufgrund ihrer Handelsbeziehungen mit europäischen Unternehmen den Regularien der DSGVO angepasst. Viele nutzten beispielsweise Cookie-Banner mit Opt-Out, obwohl nach bisherigem Schweizer Recht diese Zustimmung noch gar nicht nötig wäre. Und auch die Zahl der Datenschutzbeauftragten nehme stetig zu, obwohl es im neuen Gesetz keine Verpflichtung zur Ernennung eines Datenschutzbeauftragten geben werde.

Vladan Rámiš, Vorstandsvorsitzender des Vereins für Schutz von personenbezogenen Daten, sieht die DSGVO mehr als Weg denn als Ziel. „Datenschutz ist ein Prozess, der immer läuft“, sagte er. In Tschechien sei die Umsetzung der DSGVO noch in vielen Betrieben in vollem Gange, ähnliches schildert Philipp Mittelberger aus Liechtenstein. In beiden Ländern gibt es keine gesetzliche Verpflichtung ab einer bestimmten Firmengröße einen Datenschutzbeauftragten ernennen zu müssen. Liechtenstein allerdings, das zeigt der Beitrag der Datenschutzbeauftragten von Liechtenstein, Marie-Louise Gächter, in dieser Ausgabe, hat sich selbst an der DSGVO und vor allem am BDSG orientiert.

## Datenschutz praktisch

Daneben gab es wieder viele Vorträge zu technischem Datenschutz und praktischen Anwendungen, zum Beispiel von Thomas Kahl zum aktuellen Thema Gesundheitsdaten oder von BvD-Vorstand Dr. Christoph Bausewein und Chris Meidinger zur Bedrohungslage und Verteidigungsstrategien im Internet. Carlo Piltz griff die Diskussion um die Rolle von Rechtsanwälten als Datenschutzbeauftragte auf, und der Datenschutzanwalt Tim Wybitul sowie Maria Christina Rost, Leiterin der Stabstelle Justiziariat beim Hessischen Beauftragten für Datenschutz und Informationsfreiheit, widmeten sich dem Thema Bußgelder durch die Aufsichtsbehörden.

Zum Imbiss aus unserem Snack-Pack, das alle Teilnehmenden pünktlich zum Start der dreitägigen Veranstaltung per Post nach Hause erhielten, konnten sich alle Interessierten auf unserer Big-Blue-Button-Plattform vernetzen, austauschen und Fragen zum Beispiel an unsere Partner, die Aufsichtsbehörden von Brandenburg, Berlin und Niedersachsen stellen.

## Tipps und Tools der Event Partner

Besonders hervorzuheben ist auch das Engagement der Event-Partner, die mit Vorträgen und Beratungen in der Event Partner Lounge viele Tipps und Tools für die Datenschutz-Praxis präsentierten.

Andreas Beck, Datenschutz-Berater beim Unternehmen OneTrust, dessen Cookie-Banner auf vielen Internetseiten zum Einsatz kommen, referierte zum Thema globaler Datenschutz, audatisManager-Gründer und Geschäftsführer Carsten Knoop gab hilfreiche Impulse für die Lösch- und Aufbewahrungsfristen in Behörden und Manfred Gerber, Leiter des Geschäftsbereichs Privacysoft beim Unternehmen Projekt29, beriet, wie sich eine Datenschutzmanagement-Software systematisch planen und steuern lässt. Weitere Eventpartner waren TeachToProtect, IITR, Rhenus Office Systems und jbv Jared Butz.

Auch wenn sich die meisten wohl auf eine reale Präsenzveranstaltung gefreut hatten, zeigte sich, dass die virtuelle Begegnung nicht weniger intensiv sein muss. Rund 300 Teilnehmende beweisen das. Sie alle virtuell und ohne nennenswerte Technikprobleme zu erreichen ist natürlich auch eine logistische Herausforderung, die nur gemeinsam mit der BvD-Geschäftsstelle, mit verlässlichen Partnern und mit viel Kraft und und manchem nächtlichen Einsatz gestemmt werden konnte.

Die BvD-Herbstkonferenz 2021 wird bei abflauender Pandemie als Hybrid-Veranstaltung im Oktober in Nürnberg geplant. Dabei kann sich eine begrenzte Zahl von Teilnehmenden vor Ort anmelden, andere können sich wieder per Online-Plattform zuschalten und die Vorträge und Diskussionen vom Büro oder dem Homeoffice aus verfolgen. Anmeldungen sind bereits jetzt über die BvD-Website möglich. Dort finden sich auch detaillierte Informationen zum Kongressprogramm.

Über den Autor

**Jürgen Hartz**

ist BvD-Vorstandsmitglied und zuständig für Veranstaltungen

**Hybrid-Veranstaltung**

begrenzte Plätze für Präsenz-Teilnahme

2021

# BvD-Herbstkonferenz Datenschutz & Behördentag

**27.10. - 29.10.2021 im Hotel NH München Ost Conference Center**

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.

## WIRTSCHAFT TRIFFT AUFSICHT

DIGITALISIERUNG GESTALTEN: HERAUSFORDERUNGEN DER MODERNEN ARBEITSWELT

**MIT FOLGENDEN THEMEN:**

- Digitalisierung & Beschäftigtendatenschutz
- Drittlandtransfers & neue Standarddatenschutzklauseln
- Herausforderungen des Datenschutzes im Jahr 4 der DSGVO
- Art. 82 DSGVO - Lizenz zum „Geld drucken"?
- Art. 6.1.f DSGVO - (k)ein „Persilschein" für alles
- Bußgeldpraxis & Gerichtsentscheidungen

**JETZT ANMELDEN:**

www.bvdnet.de/herbstkonferenz-datenschutz

**Gemeinsame Konferenz von:**

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg

BayLDA

BvD e.V. DATENSCHUTZ GESTALTEN

# DATENSCHUTZ: DAS SALZ IN DER SUPPE DER DIGITALISIERUNG

Prof. Ulrich Kelber

Wir Deutschen haben bekanntlich die teuersten Küchen und das billigste Essen. Dieses Verhältnis wird sich vermutlich nicht ändern lassen. Wenn nun aber der Herd kaputt geht, lässt sich erst recht keine schmackhafte Suppe zubereiten. In der Küche unserer Gesellschaft bekommen wir genau das gerade schmerzhaft zu spüren. Die aktuelle Krise zeigt auch über ihre unmittelbare Bewältigung hinaus ganz klar die vielen Versäumnisse und Defekte, die nicht erst mit der Pandemie entstanden sind. Das gilt vor allem für die lahmende Digitalisierung. Über Jahre kaputtgesparte Gesundheitsämter versuchen mit altertümlichen Faxgeräten tagesaktuelle Inzidenzzahlen zu melden. Bildungsplattformen brechen zusammen, weil die Server nie für den Fernunterricht aller Schülerinnen und Schüler ausgelegt waren. Und ein Teil der Verwaltung saß tatenlos im Homeoffice, weil er weder mobile dienstliche IT noch eine sichere Verbindung hatten.

Die Pandemie und ihre Bewältigung stellt uns alle vor Herausforderungen, die wir in dieser Form noch nicht erlebt haben. Trotzdem sind sie sichtbar, denn sie beeinflussen unseren Alltag massiv. Weniger wahrnehmbar sind hingegen die tektonischen Veränderungen auf den internationalen Märkten. Hier erleben wir gegenwärtig einen enormen Zuwachs der Wirtschaftsmacht der großen internationalen Technologiekonzerne. Der unumkehrbare pandemiebedingte Digitalisierungsschub spielt ihnen dabei noch mehr in die Hände. Was in der Krise mit Hochdruck gekommen ist, wird auch mit der für Spätsommer oder Herbst erhofften Herdenimmunität nicht wieder verschwinden. Dem mobilen Arbeiten und der Nutzung digitaler Techniken gehört die Zukunft.

Die betriebliche Arbeitswelt befindet sich schon länger mitten in der digitalen Transformation. Diese wiederum hat gravierende Auswirkungen auf unsere Art zu wirtschaften, zu arbeiten und auch zu leben. Betriebe stehen vor schwierigen und sehr komplexen Problemen. Sie müssen neue digitale Geschäftsmodelle entwickeln und neue Märkte erschließen. Dabei muss der Einsatz digitaler Hilfsmittel schneller und effizienter werden.

Aufgrund der Fixierung auf Verfügbarkeit und Geschwindigkeit kommen die Probleme des Schutzes der personenbezogenen Daten sowie der Datensicherheit oftmals zu kurz. Dabei sind sie für die innerbetriebliche Akzeptanz wie auch für die Gewinnung von Kunden von großer Bedeutung. Viele Akteure sind auf diese technologischen Paradigmenwechsel alles andere als gut vorbereitet. Gerade wegen der allgemeinen Unsicherheit ist es wichtig, dass wir uns auf bestimmte Standards verlassen müssen. Da darf es keine Wanken und Wackeln geben. Für betriebliche und behördliche Datenschutzbeauftragte bedeutet das zukünftig noch mehr Verantwortung. Dazu gehört auch, dass wir zwingend die „neuen" Arbeitsformen unserer Zeit jenseits der Tätigkeit im Betrieb oder der Behörde mitdenken müssen.

Gerade deshalb kommt den Datenschutzbeauftragten in Unternehmen und Verwaltungen eine Schlüsselrolle zu.

Sie werden die Lotsen für die Entwicklung und vor allem für die Einführung neuer digitaler Technologien. Doch erkennen Wirtschaftsverbände und Politik diese Notwendigkeiten? Da habe ich meine Zweifel. Ebenso wie bei der Evaluierung des Bundesdatenschutzgesetzes. Die Schwächung der Unternehmen durch die Aushöhlung der Benennungspflicht ist eine Rolle rückwärts. Der Umfang der Datenverarbeitung und deren Brisanz hängen doch nicht von der Zahl der Beschäftigten ab.

Dass der Gesetzgeber die Grenze der Benennungspflicht an der Zahl der Mitarbeiter festmacht, geht an der Wirklichkeit vorbei. Er hängt allem Anschein nach noch immer im Zeitalter der Papierakten fest. Ich teile die Auffassung, dass der Gesetzgeber die Einbindung der Datenschutzbeauftragten in die Gestaltung der Verarbeitung personenbezogener Daten stärken sollte. Sie müssen beispielsweise die Möglichkeit haben die Unternehmensleitung bei bestimmten Verpflichtungen nach der DSGVO auch zu entlasten. Das käme im Übrigen gerade kleinen und mittleren Unternehmen zu Gute. Ich kann nur hoffen, dass die Politik den Nutzen eines Datenschutzbeauftragten und dessen Know-how erkennt und für die Unternehmen besser nutzbar macht.

Und ich hoffe, dass die Politik sich der Tragweite ihrer Entscheidungen bewusst ist. Ob die Schließung ganzer Gewerbebereiche, nächtliche Ausgangssperren oder die Beschränkung der Reisefreiheit: Unsere Grundrechte stehen momentan unter einem bisher nie dagewesenen Rechtfertigungsdruck. Es ist generell, gerade in Krisenzeiten, für die Exekutiven immer verführerisch Grundrechte zu verkürzen. Trotzdem bin und bleibe ich zuversichtlich, dass die Grundrechtsordnung nicht unter die Räder der Pandemie gerät.

Die geplanten Maßnahmen müssen stets auf ihre Eignung und ihre Erforderlichkeit überprüft werden. Besonders stark freiheitseinschränkende Maßnahmen müssen nach Krisenende wieder zurückgenommen werden. Das haben Gerichte immer wieder so entschieden. Aus datenschutzrechtlicher Sicht gab es im Übrigen bei dieser Herausforderung grundsätzlich keine wirklichen unlösbaren Probleme. Keine einzige geeignete und effektive Maßnahme zur Pandemiebekämpfung ist am Veto der Datenschutzaufsicht gescheitert!

Das hat natürlich trotzdem viele nicht davon abgehalten öffentlich rum zu jammern, dass durch den bösen Datenschutz die Volksgesundheit den Bach runter geht. Es wird immer mehr mit dem Bauchgefühl hantiert. Weder Talkshow-Philosophen noch Medien mit hoher Reichweite und eigentlich gutem Ruf fühlen sich genötigt ihre persönliche Ansicht durch Fakten zu begründen. Hauptsache, die Position passt in die vermeintliche Gefühlslage der Nation. So wurde beispielsweise, durch eine leider nicht kleine Gruppe von Politikern, Wirtschaftsvertretern und sogar Wissenschaftlern – teilweise wider besseren Wissens – beharrlich erzählt, dass der Datenschutz das einzige Grundrecht sei, das unangetastet fortbestehe. Das ist natürlich vollständiger Unsinn, denn wie andere Grundrechte wurde auch der Datenschutz – und zwar zu Recht – zur Pandemiebekämpfung eingeschränkt. Denken wir nur an die Kontakterfassungen bei Reiserückkehrern oder in der Gastronomie und im Einzelhandel. Dass Datenschutz unberechtigterweise zum Sündenbock gemacht wird, ist leider nichts Neues. Gestern war er Wirtschaftshemmnis, heute hindert er die Pandemiebekämpfung, morgen wieder den Kampf gegen Kriminelle. Die Bürgerinnen und Bürger sind an dieser Stelle zum Glück viel weiter, denn in allen offen formulierten Umfragen wünschen sie sich mehr Datenschutz und nicht weniger.

Das gilt insbesondere für ihre besonders sensiblen Gesundheitsdaten. Die Datenschutz-Grundverordnung verlangt deshalb geeignete Garantien zum Schutz der betroffenen Personen. Bei der Corona-Warn-App konnte man sehen, wie Transparenz und datenschutzfreundliche Entwicklung zu hohem Vertrauen der Nutzenden führen. Doch anstatt diesen eher zufälligen Erfolg als Musterbeispiel für eine intelligente Digitalisierung zu nehmen wurde Datenschutz in der öffentlichen Diskussion mehr und mehr zum Punchingball. Wer aber hat denn die Gesundheitsämter kaputt gespart, in der Pflege das Personal gekürzt und keine einheitlichen IT-Systeme eingeführt? Das war nicht der Datenschutz.

Während sich also alle Welt mit angeblich störendem Datenschutz in der Pandemie beschäftigt, ist die datenschutzrelevante Gesetzgebung andernorts keineswegs stehen geblieben. Alte Probleme, gerade im Sicherheitsbereich, warten weiter auf eine rechtsstaatliche Lösung. Und wenn es neue Gesetzesentwürfe gibt, werden die Befugnisse der Sicherheitsbehörden auf Vorrat größtmöglich ausgebaut und erst dann wieder enger gefasst, wenn das Bundesverfassungsgericht dies verlangt. Das wird im Übrigen beim Infektionsschutzgesetz ähnlich ablaufen. Auf Corona zugeschnittene Befugnisse der Exekutive, die nicht mit der Pandemie automatisch verfallen, bleiben bis zum jüngsten Tag dort bestehen. Echte Evaluationen finden fast nie statt. Der Datenschutz darf diese Dinge nicht vom Rand her beklagen. Er muss vielmehr seinen energischen Beitrag leisten diese technischen und rechtlichen Nachholprozesse in die richtige Richtung zu lenken. Eines lasse ich den Verantwortlichen allerdings nicht durchgehen. Wenn sie nunmehr gezwungen sind, teilweise schnell neue Lösungen zur Behebung des Digitalisierungsdefizits zu präsentieren, können sie sich nicht hinter der Pandemie verstecken und ausschließlich auf datenschutzfragwürdige Produkte setzen, einzig weil sie von weiten Teilen der Bevölkerung ohnehin schon genutzt wer-

den. Es gibt alternative datenschutzfreundliche Angebote am Markt. Ich sehe in der Krise eine – vielleicht letzte – Chance für die Wirtschaft endlich mit datenschutzfreundlichen Lösungen zu punkten. Der Markt hat noch immer zu wenig im Angebot, um die riesige Nachfrage zu befriedigen. Wer hier vorangeht wird schnell merken: Datenschutz ist auch gut für die Bilanzen. Die Einhaltung der entsprechenden Gesetze leistet einen Beitrag zur Wahrung der Freiheit in der demokratischen Gesellschaft. Die DSGVO ist gewiss nicht vollkommen. Aber immer mehr Staaten nehmen sie sich zum Vorbild, zum Beispiel Indien, Brasilien, Japan oder Singapur.

Digitalisierung darf nie zum Selbstzweck werden. Jeder technische Fortschritt hat vielmehr dem Menschen zu dienen. Wir sollten gemeinsam dafür sorgen, dass der Datenschutz gerade auch bei den Digitalisierungsprojekten endlich von Anfang an mitgedacht wird. Als Deutsche und als Europäer stehen wir für eine andere Digitalisierung als autoritäre Überwachungsregimes wie z.B. in China oder Laissez-faire-Ansätze wie in den USA.

Um das Bild vom Anfang aufzugreifen: Denken wir daran, dass wir nicht mehr nur in der kleinen deutschen Kochnische stehen, sondern in einer europäischen Großküche. Es wird Zeit, dass wir den digitalen Herd reparieren und endlich anfangen unsere Zukunft zuzubereiten. Sorgen wir dafür, dass es zur Selbstverständlichkeit wird beim Begriff der Digitalisierung automatisch auch an Datenschutz zu denken, oder – sogar noch besser: Sorgen wir dafür, dass man beim Thema Digitalisierung gar nicht mehr über Datenschutz reden muss, weil er als essentieller Bestandteil ohnehin immer dazu gehört.

**Denn eine Sache weiß jeder: Suppe ohne Salz schmeckt einfach nicht!**


Über den Autor

**Prof. Ulrich Kelber**
ist seit 2019 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit.

▶ www.bfdi.bund.de

BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

# DATENSCHUTZKONFORMITÄT HERSTELLEN

## Mit Abflauen der Pandemie müssen rechtswidrige Zustände behoben werden

Maja Smoltczyk

In einer demokratischen und den Grundrechten verpflichteten Gesellschaft kann die Digitalisierung ohne Datenschutz nicht funktionieren. Das Recht auf informationelle Selbstbestimmung ist ein über viele Jahre entwickeltes Grundrecht. Die Erkenntnis, dass in Zeiten einer immer weiter fortschreitenden Digitalisierung aller Lebensbereiche eine totale Ausforschung der Menschen verhindert werden muss, um private, unbeobachtete Bereiche zu erhalten und damit die Möglichkeit sich frei als Persönlichkeit zu entfalten, hat letztlich zur Entwicklung der europäischen Datenschutz-Grundverordnung geführt. Denn in Zeiten globaler Vernetzung sowie rasanter Ausbreitung algorithmischer Verfahren und künstlicher Intelligenz können Nationalstaaten allein die europäischen Grundrechte nicht in die Zukunft retten.

Europa hat mit der Schaffung eines europaweit einheitlichen Datenschutzrechts Maßstäbe gesetzt. Damit aber die Regeln der Datenschutz-Grundverordnung eingehalten werden, muss es Aufsichtsbehörden geben, die die Einhaltung der Regeln kontrollieren. Es muss aber vor allem auch vor Ort Personen geben, die im täglichen Arbeitsbetrieb darauf achten, dass das Recht auf informationelle Selbstbestimmung ernst genommen und beim Einsatz der verwendeten Technologien und Verfahren miteinbezogen wird. Und genau dies ist die Aufgabe der Datenschutzbeauftragten vor Ort, also der behördlichen und betrieblichen Datenschutzbeauftragten.

Die Digitalisierung ist ein komplexer und für die meisten Menschen weitgehend undurchschaubarer Prozess. Gerade im Bereich der öffentlichen Verwaltung muss besonders auf die Einhaltung der datenschutzrechtlichen Regeln geachtet werden. Denn wir leben in einer Zeit, in der das Misstrauen Staat und Politik gegenüber wächst. Der Umbau der Verwaltung kann nur gelingen, wenn dabei das Vertrauen der Bürgerinnen und Bürger nicht verloren geht. Und dieses Vertrauen ist nur zu wahren, wenn die Menschen sich darauf verlassen können, dass einerseits ihre Daten sicher sind und andererseits größtmögliche Transparenz über die Verarbeitung der Daten und die Ziele des staatlichen Handelns hergestellt wird.

Durch die Corona-Pandemie mit ihren immensen Auswirkungen auf die gesamte Gesellschaft hat die Digitalisierung einen völlig unerwarteten Schub erlebt. Die teils überstürzte Digitalisierung, vor allem im Bereich von Bildung und Arbeit, führte leider dazu, dass vielfach Produkte zur Anwendung kamen, die den datenschutzrechtlichen Anforderungen nicht entsprachen. Wir Aufsichtsbehörden haben in dieser außergewöhnlichen Situation weitgehend von Sanktionen abgesehen, da es in dieser Zeit darum ging das gesellschaftliche und wirtschaftliche Leben irgendwie aufrechtzuerhalten. Wir haben aber immer wieder darauf hingewiesen, dass dies kein Dauerzustand sein kann.

In dieser Zeit haben wir gesehen, welche Möglichkeiten die Digitalisierung bietet, zugleich haben wir aber auch erlebt, wie vieles noch im Argen liegt, welche Probleme dringend gelöst werden müssen und wieviel Handlungsbedarf es an den meisten Stellen noch gibt. Und genau da stehen wir jetzt. Mit Abflauen der Pandemie geht es nun darum nachzuarbeiten und die rechtswidrigen Zustände zu beseitigen. Produkte und Datenverarbeitungsverfahren müssen auf ihre Datenschutzkonformität geprüft und nachgebessert oder ausgetauscht werden.

Hier werden die Datenschutzbeauftragten gefordert sein. Denn beim Datenschutz geht es nicht um ein Luxusgut, sondern um ein Grundrecht, und es geht um die Einhaltung gesetzlicher Anforderungen. Dies müssen wir uns immer wieder vor Augen führen. Wir haben erlebt, wie in der Zeit der Pandemie immer wieder versucht wurde den Datenschutz als zentrales Problem hinzustellen. Es wurde suggeriert, dass der Datenschutz nur eingeschränkt werden müsste, dann ließen sich nahezu sämtliche Herausforderungen der Pandemie leichter lösen. Fast jeden Tag hörte man: Der Datenschutz hält unsere Kinder vom Lernen ab! Der Datenschutz steht dem Homeoffice im Wege! Der Datenschutz behindert die Gesundheitsämter bei der Pandemiebekämpfung! Dies zu behaupten war natürlich leichter als sich auf die Suche nach den wahren Problemen zu begeben. Problematisiert wurde nicht, dass die Gesundheitsämter noch immer nicht alle an die digitale Infrastruktur angeschlossen sind.

Problematisiert wurde auch nicht, dass die Ämter mit den Daten von Corona-Kontaktlisten bereits überfordert waren, wenn eifrig gefordert wurde, die App müsste noch viel mehr Daten sammeln. Problematisiert wurde nicht, dass kaum ein kommerzieller Anbieter datenschutzgerechte Lösungen anbietet und Behörden nicht in der Lage sind solche Lösungen selbst zu entwickeln oder entsprechende Lösungen in Ausschreibungen einzufordern. Problematisiert wurde auch nicht, dass US-amerikanische Dienste es sich vorbehalten wollen die Daten von Kindern zum Beispiel durch Lernangebote an Schulen für eigene, meist kommerzielle, Zwecke zu verarbeiten. Behauptet wird stattdessen, dass die Datenschützer*innen den Kindern das Lernen verbieten wollen.

Ich kann allen versichern: Nein, das wollen wir nicht!

Was wir allerdings wollen, ist, dass unsere Kinder in einer sicheren Umgebung aufwachsen, in einem geschützten Raum, in dem sie lernen können mit den Gefahren der Digitalisierung umzugehen und sich keine Sorgen zu machen brauchen, dass ihre Lernerfolge oder -misserfolge ihnen vielleicht noch nach Jahren vorgehalten werden könnten ebenso wie vielleicht unbedachte Äußerungen im Politik- oder Ethik-Unterricht, die auf einmal zu unerwarteten Schwierigkeiten bei späteren Reisen oder bei der Jobsuche führen könnten.

Gerade im schulischen Kontext spielt der Datenschutz eine sehr wichtige Rolle. Nicht umsonst stellt die Datenschutz-Grundverordnung Kinder und Jugendliche unter einen besonderen Schutz. Digitale Lernplattformen bergen ein nicht zu unterschätzendes Gefahrenpotenzial: Sie verlangen eine personalisierte Anmeldung, erheben teilweise völlig unnötige Daten, haben nicht immer ausreichende Löschfunktionen und können häufig das Nutzungsverhalten sehr genau auswerten. Dies wird zu einem erheblichen Problem insbesondere dann, wenn die anbietenden Unternehmen ihren Sitz außerhalb der Europäischen Union haben und sich die Durchsetzung europäischen Datenschutzrechts schwierig gestaltet.

Aber auch in vielen anderen Bereichen waren die Herausforderungen durch die Pandemie groß. So musste auf einmal ein Großteil der Arbeit nach Hause verlegt werden. Das warf viele datenschutzrechtliche Fragen auf, mit denen die Datenschutzbeauftragten in Unternehmen und in der Verwaltung plötzlich umgehen mussten: Wie sensibilisieren wir unsere Mitarbeiter*innen für den Umgang mit personenbezogenen Daten im Homeoffice? Wie stellen wir sicher, dass unsere Mitarbeiter*innen von zu Hause aus datenschutzkonform arbeiten können? Welche Endgeräte, Videokonferenztools und Software setzen wir dabei ein? Das alles sind Fragen, die ad-hoc nicht einfach zu beantworten waren und viele Behörden völlig unvorbereitet trafen.

In unserer Aufsichtspraxis haben wir aber deutlich gemerkt, dass viele Menschen sich durchaus sehr viele Gedanken über den Schutz ihrer persönlichen Daten machen und sehr verunsichert sind angesichts der derzeit so rasanten Digitalisierungswelle. Die vielen Anfragen und Beschwerden, die meine Behörde erreichen, zeichnen da ein deutliches Bild. Insbesondere zu Beginn der Corona-Pandemie zeigte sich schnell, dass die Verunsicherung in Bezug auf Videokonferenzlösungen und durch Schulen genutzte digitale Lernplattformen immens war. Wir haben daher getan, was wir konnten, um mit Veröffentlichungen auf die dringendsten Fragen einzugehen und Hilfestellung zum datenschutzkonformen Einsatz digitaler Mittel zu geben. Vor allem haben wir eine Prüfung der gängigsten Videokonferenzdienste durchgeführt und veröffentlicht, um in diesem Bereich die dringend benötigte Orientierung zu geben.

Es ging uns dabei darum aufzuzeigen, welche datenschutzkonformen Produkte es auch jetzt schon gibt und wo vielleicht auch heute schon nachgebessert werden kann. Unsere Prüfung hat dann dazu geführt, dass einige der Unternehmen erhebliche Nachbesserungen an ihren Produkten vorgenommen haben und die Zahl datenschutzkonformer Produkte erfreulich steigt.

Es ist daher weder unangemessen noch unrealistisch jetzt die Umstellung auf datenschutzgerechte Produkte und Verfahren zu fordern. Schulen zum Beispiel müssen sich zum Schutz der Kinder umstellen. Natürlich können sie dies nicht allein, denn die Auswahl entsprechender Angebote ist eine technisch und rechtlich hochkomplexe Aufgabe, die weit über pädagogische Erwägungen hinausgeht und für die weder Schulleitungen noch Lehrkräfte ausgebildet sind. Hier sind die übergeordneten Verwaltungen gefordert entsprechende Rahmenbedingungen zu schaffen.

Und auch wenn dies eine große Herausforderung nicht nur für die Schulen, sondern für alle gesellschaftlichen und wirtschaftlichen Bereiche ist, kommen wir doch daran nicht vorbei. Der Europäische Gerichtshof hat in seiner Schrems-II-Entscheidung festgestellt, dass die weitreichenden Zugriffsmöglichkeiten von US-Behörden auf Daten europäischer Bürger*innen nicht mit dem europäischen Datenschutzrecht im Einklang stehen, und hat das „EU US Privacy Shield“ als bis dahin verwendete Grundlage für Übermittlungen personenbezogener Daten in die USA gekippt. Personenbezogene Daten

dürfen demnach grundsätzlich nicht mehr oder nur unter sehr engen Voraussetzungen in die USA übermittelt werden. Vor dem Hintergrund, dass der Großteil der europäischen Datenverarbeitung bisher auf Produkten der großen amerikanischen Technologie-Unternehmen basierte, wird klar, welchen Herausforderungen wir derzeit tatsächlich gegenüberstehen.

Es geht um nichts weniger als um die Schaffung einer europäischen Souveränität im Bereich der Datenverarbeitung.

In allen Bereichen sind wir jetzt gefordert. Wir hatten uns das nur noch nicht so richtig klargemacht. Die Pandemie hat nun wie durch ein Brennglas auf die vor uns liegenden Baustellen hingewiesen. Die während der Pandemie gemachten Erfahrungen sollten daher als Ansporn dafür genommen werden die Digitalisierung neu und nachhaltig zu gestalten. Der Datenschutz muss von Anfang an mitgedacht werden, nur so kommen wir zu vertrauenswürdigen Produkten und Verfahren. Und dabei muss und kann nicht alles selbst entwickelt werden, wenn die Rahmenbedingungen stimmen. Die Verwaltung muss sich dessen bewusst sein, dass sie auch eine nicht zu unterschätzende Wirtschaftsmacht darstellt, die Forderungen erheben kann und sollte. Ausschreibungen in der öffentlichen Verwaltung müssen so formuliert werden, dass die Anforderungen des Datenschutzes eingefordert werden. Unsere Erfahrung als Aufsichtsbehörde ist, dass sich da Vieles bewegen kann. Und daher möchte ich die Datenschutzbeauftragten ermuntern: Helfen Sie mit Ihrer Expertise tatkräftig mit und lassen Sie sich trotz gelegentlicher Widerstände nicht entmutigen, denn aus eigener Erfahrung kann ich sagen: Die Mühe ist es wert!

Über die Autorin

**Maja Smoltczyk**
ist seit Januar 2016 Berliner Beauftragte für Datenschutz und Informationsfreiheit.

# DATENSCHUTZ ALS DATA GOVERNANCE

Dr. Nikolai Horn

## 1. Datenschutz als Innovationsbremse?

Folgende Situation dürfte vielen Datenschutzbeauftragten bekannt vorkommen: Das Projektteam setzt einen Datenverarbeitungsprozess auf oder entwickelt ein digitales, datenbasiertes Produkt. Erst gegen Ende des Entwicklungsprozesses fällt den Projektverantwortlichen ein, dass man vielleicht auch nochmal nachprüfen müsste, ob datenschutzrechtlich alles in Ordnung ist. Wenn man an dieser Stelle die Datenschutzbeauftragen hinzuzieht und diese Einwände oder Hinweise hervorbringen, werden sie schnell zum Buhmann oder zur Buhfrau. Datenschutz hat mit seinem Ruf als etwas, das für „Bedenkentum" steht, zu kämpfen und das Klischee, er sei nur eine lästige „Innovationsbremse", verfestigt sich.

Dabei ist das eigentliche Problem nicht der Datenschutz, sondern vielmehr die nicht (oder kaum) vorhandene Datenkultur. Gerade bei innovativen Unternehmen ist der strategische Umgang mit Daten noch eine große Herausforderung. In eine Datenschutzkultur ist die rechtskonforme Verarbeitung personenbezogener Daten ein Teil eines ganzheitlichen Data Governance Prozesses. Anforderungen im Zusammenhang mit Aspekten wie Datenqualität, Metadatenmanagement oder Rollenkonzept werden von vornherein mitgedacht.

Doch was ist unter Data Governance genau zu verstehen? Welchen Stellenwert hat der Datenschutz innerhalb einer entsprechenden Strategie? Und wie können Organisationen dazu befähigt werden, einzelne Data Governance Themen frühzeitig und strukturiert anzugehen?

## 2. Was ist Data Governance?

In der Datenstrategie der Bundesregierung wird Data Governance als „Rahmenbedingungen (Gesetze, Verordnungen, Standards, interne Regelungen) und organisatorische Strukturen in Bezug auf das Management (die Verwaltung und Nutzung) von Daten in Behörden, Unternehmen oder anderen Entitäten"[1] beschrieben. In diesem Sinne ist Data Governance ein Prozess zur Umset-

[1] Datenstrategie der Bundesregierung, S. 107.

zung von Anforderungen und Normen im Umgang mit Daten durch bestimmte technisch-organisatorische Maßnahmen in einzelnen Themenbereichen.

Diese Themenbereiche sind vielfältig. Neben Datenschutz handelt es sich dabei um Themen wie:

**Metadatenmanagement:** Metadaten sind strukturierte Daten, die Informationen über andere Daten beschreiben. Sie bilden den Grundbaustein für die Funktionsfähigkeit von Datenverarbeitungsprozessen.

**Rollenkonzept:** Für den Betrieb der Datenverarbeitungssysteme ist die Identifikation und Zuweisung von Rollen und Verantwortlichkeiten sehr wichtig. Beim Rollenkonzept wird geklärt, wer die Gesamtverantwortung für die Datenverarbeitung trägt, wer für welche Umsetzungsschritte zuständig ist und welche internen und externen Stakeholder mit involviert werden sollen.

**Datenqualität:** Daten werden als qualitativ hochwertig angesehen, wenn sie für ihren vorgesehenen Gebrauch im operativen Geschäft geeignet sind. Datenqualität beschreibt damit die Korrektheit, die Relevanz und die Verlässlichkeit von Daten, abhängig vom Zweck, den sie in einem bestimmten Zusammenhang erfüllen sollen.

**Datensicherheit:** Datensicherheit bezeichnet die technischen und organisatorischen Maßnahmen, die notwendig sind, um je nach Schutzbedarf der Daten und datenverarbeitenden Systeme ein angemessenes Schutzniveau zu gewährleisten.

**Datenethik:** Datenethik beschäftigt sich mit der Anwendung einzelner ethischer Prinzipien und Normen auf konkrete technologische Herausforderungen. Ziel ist dabei die Schaffung der relevanten Voraussetzungen, die auf die Einhaltung bestehender (grund-)rechtlicher Rahmenbedingungen und ethischer Prinzipien abzielen.

Jedes der aufgeführten Themen ist, wie auch der Datenschutz, für sich genommen anspruchsvoll und erfordert den Einsatz fachlich geschulter Spezialist:innen. Zugleich bestehen aber zwischen all diesen Themen enge Wechselbeziehungen, die in ihrer Gesamtheit eine umfassende Data Governance ausmachen. Ein Blick auf den Datenschutz macht es deutlich:

So ist beispielsweise das Metadatenmanagement sowohl für die Sicherung der Datenqualität als auch für die Erfüllung von Datenschutzanforderungen an Datenminimierung, Zweckbindung oder Datenrichtigkeit entscheidend. Auch das Rollenkonzept spielt für die Erfüllung von Datenschutzanforderungen eine wichtige Rolle, um beispielsweise Zugriffsberechtigungen auf personenbezogene Daten zu regeln. Die Datenqualität ist zugleich für die Erfüllung der Datenschutzanforderung der Datenrichtigkeit entscheidend und die Datensicherheitsaspekte sind ein wesentlicher Teil für die Erfüllung der Datenschutz-Gewährleistungsziele „Vertraulichkeit", „Integrität" und „Verfügbarkeit". Ebenso sind viele digitalethische Grundsätze wie Risikofolgenabschätzung, Schadensverhütung und Nachvollziehbarkeit von datenverarbeitenden Anwendungen mit datenschutzrechtlichen Anforderungen wesensverwandt.

Diese Wechselwirkung zwischen Datenschutz und anderen Data-Governance-Aspekten spiegelt den ganzheitlichen Charakter der Digitalisierung wider. Data Governance ist dabei als ein umfassender Prozess zu verstehen, der mehrere miteinander verzahnte Einzelbereiche (Datenschutz, IT-Sicherheit, Datenethik, Datenqualität, Datenmanagement, etc.) umfasst und sie in ihrem Zusammenhang begreift.

## 3. Datenschutz als Data Governance

Das Verständnis des Datenschutzes als Teil einer ganzheitlichen Data Governance macht deutlich, warum die Auseinandersetzung damit bei digitalen Projekten von vornherein, und zwar themenübergreifend, mitgedacht werden sollte: So muss beispielsweise die Datenverarbeitung nach dem Datenschutz-Grundsatz der Richtigkeit erfolgen. Gleichzeitig ist „Richtigkeit" auch eine Anforderung im Sinne der Datenqualität und der Datenethik.

Damit die Daten korrekt bleiben, müssen sie durch IT-Sicherheitsmaßnahmen vor unberechtigten Zugriffen und Manipulationen abgesichert sein. Um die Richtigkeit der Daten regelmäßig kontrollieren zu können und bei Bedarf zu berichtigen, muss bereits ein klares Rollenkonzept mit Zugriffsrechten, Vertretungsregeln etc. vorliegen. Und ohne ein strukturiertes Metadatenmanagement ist ein Abgleich von Datendubletten und eine Vollständigkeitsprüfung von Angaben kaum zu bewältigen. Würde man die Erfüllung von Datenschutzanforderungen als einen isolierten Bereich betrachten, der aus-

schließlich der Zuständigkeit der Datenschutzbeauftragten obliegt, wird man weder dem Datenschutz noch den Innovationspotenzialen der Digitalisierung gerecht.

Man kann kaum alle Datenschutzanforderungen erfüllen ohne sich mit weitläufigen Data-Governance-Themen zu befassen. Eine späte Einbindung der Datenschutzexpert:innen hat zur Folge, dass Synergieeffekte ungenutzt bleiben und unter Umständen kostenintensive (und bei einer rechtzeitigen Einbindung unnötige) Nachbesserungen beispielsweise bei der Datenbankarchitektur vorgenommen werden müssen.

Wer erst im Nachhinein Einschätzungen zum Datenschutz einholt, handelt ineffizient. Denn: Der Umsetzungsaufwand einer nachträglichen Data Governance ist teuer, bindet Ressourcen und kann Synergien, die sich durch ein geplantes Aufsetzen ergeben, selten nutzen. Frühzeitige, strukturierte Data-Governance-Prozesse sind also nicht nur für die Erfüllung von rechtlichen Anforderungen und gesellschaftlichen Erwartungen an werteorientierte Datenverarbeitung zentral, sondern auch für eine effiziente und effektive Funktionalität der Datenverarbeitungsprozesse.

Zudem kann sich die Umsetzung von Datenschutzanforderungen auch als Katalysator für die notwendige Auseinandersetzung mit Data Governance Themen auswirken.

So nahmen viele Großunternehmen das Inkrafttreten der DSGVO zum Anlass ihre Dateninfrastruktur zu sanieren und zu erneuern: Datenflüsse zwischen unterschiedlichen Unternehmensbereichen wurden modernisiert, Datenbestände in CRM-Datenbanken bereinigt und aktualisiert sowie IT-Sicherheitsmaßnahmen auf den neuesten Stand gebracht.

Auch die Entwicklung der Corona-App unter der beratenden Begleitung durch den Bundesdatenschutzbeauftragten machte deutlich, dass die Effizienz der digitalen Innovationen weniger am Datenschutz, sondern vielmehr an der unausgebauten IT-Infrastruktur hakt.

In diesem Sinne stellt nicht der Datenschutz eine „Innovationsbremse" dar, sondern ein mangelnder Blick für die starke Interdependenz zwischen einzelnen Digitalisierungsthemen im Sinne einer ganzheitlichen Data Governance.

## 4. Der Ansatz der Self Data Governance

In der Praxis zeigt sich, dass die Entwicklung von innovativen Projekten und Geschäftsideen insofern selten strukturiert ablaufen, als Datenschutz, Datenethik und Datenqualität von vornherein nicht richtig mitgedacht werden. Viele datenbasierte Projekte sind mit dem Aufsetzen frühzeitiger, strukturierter Data-Governance-Prozesse oft überfordert.

Die Herausforderung besteht hauptsächlich darin die eigene bedarfsorientierte Auseinandersetzung mit dem Thema Data Governance strukturiert zu denken und anzugehen. Da der Rückgriff auf externe Beratungsleistungen sehr kostenintensiv werden kann, ist dies vor allem für kleinere Projekte oder KMU mit begrenzten Ressourcen oft keine Option. Vielmehr ist hierbei ein Self-Data-Governance-Ansatz gefragt, der eine eigenständige Bedarfsanalyse ermöglicht und – mitunter im Einzelfall notwendige – Rückgriffe auf externe Expertise gezielt zu steuern gestattet.

Die im April 2020 von der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder erarbeitete Methode zur Datenschutzberatung und -prüfung – das Standard-Datenschutzmodell (SDM) Version 2.0b[2] – stellt beispielsweise einen wichtigen Schritt zur Befähigung von Organisationen zu einer eigenständigen Auseinandersetzung mit dem Thema Datenschutz dar. Anhand einheitlicher Gewährleistungsziele kann es den Organisationen erleichtert werden die Erfüllung von Datenschutzanforderungen strukturiert zu steuern und Beratungsbedarfe gezielt zu identifizieren.

Ähnliche Ansätze wie die IT-Grundschutz-Methode des Bundesamtes für Sicherheit in der Informationstechnik (BSI) wären auch für weitere oben aufgezählte Data-Governance-Themen wünschenswert.

Die wesentliche Herausforderung bei solchen „Hilfen zur Selbsthilfe" besteht allerdings zum einen darin die Usability dieser Ansätze stärker zu adressieren: Mit seinen 70 Seiten ist beispielsweise die Nutzer:innenfreundlichkeit des SDM noch ausbaufähig. Auch die IT-Grundschutz-Methode des BSI dürfte für eine Erstbefassung mit dem IT-Sicherheitsthema überfordernd wirken. Zum anderen muss eine Balance zwischen der Ge-

[2] https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V2.0b.pdf

währleistung der Verständlichkeit sowie Nutzer:innenfreundlichkeit einerseits und der gebührenden Tiefe angesichts der Themenkomplexität andererseits gefunden werden. Schließlich muss im Sinne einer ganzheitlichen Data Governance gewährleistet sein, dass bei der Auseinandersetzung mit einem Themenbereich zugleich auch die weiteren Data-Governance-Themen mitbedacht werden.

Einen Schritt zur Bewältigung dieser Herausforderungen stellt das Self-Data-Governance-Framework dar, das vom Think Tank iRights.Lab im Rahmen der mFUND-Begleitforschung[3] des Bundesministeriums für Verkehr und digitale Infrastruktur (BMVI) entwickelt wurde und seit Juni 2021 frei zur Verfügung steht.[4] Dort werden beispielsweise im Themenbereich Datenschutz die sieben Gewährleistungsziele des SDM und die dazugehörigen Maßnahmen in Form einer Excel-Tabelle strukturiert dargestellt.

Es ermöglicht den Zielgruppen sich je nach Interessenstiefe über unterschiedliche Themen zu informieren, Handlungsanleitungen mit Beispielen und weiterführenden Links zu nutzen, den eigenen Data Governance Prozess zu koordinieren und den Umsetzungsstand individuell zu dokumentieren. Im Framework wurden zunächst die Themenbereiche „Datenschutz", „Datenqualität" und „Datenethik" adressiert. Dabei wird die Verwandtschaft der einzelnen Maßnahmen zwischen diesen drei Themen aufgezeigt. Die Erfüllung einer Maßnahme aus dem Bereich „Datenschutz" beispielsweise erfüllt zugleich zum Teil bestimmte Maßnahmen aus anderen Themenbereichen.

Im Hinblick auf die Usability mag eine Excel-Tabelle vielleicht nicht die optimalste Lösung sein. Perspektivisch wäre ein Open-Source-Tool wünschenswert, das alle Themenbereiche von Data Governance abdeckt, eine niederschwellige Behandlung von Data Governance Themen ermöglicht und zugleich die Data Literacy der Nutzer:innen fördert. Auf diese Weise könnte eine frühzeitige und strukturierte Einleitung von Data Governance Prozessen ermöglicht werden, die bei den beteiligten Akteuren zugleich die Lust auf die Auseinandersetzung mit diesen wichtigen Themen fördert.

[3] https://www.bmvi.de/SharedDocs/DE/Artikel/DG/mfund-projekte/self-governance-datengetriebener-innovation-begleitforschung-daten-governance.html.

[4] https://irights-lab.de/selfdatagovernance/.

## 5. Ausblick

Langfristig erfolgreiche datenbasierte Projekte und Organisationen zeichnen sich durch ein umfassendes Verständnis von digitalen Prozessen, also von Data Governance aus. Die starke Interdependenz der verschiedenen Digitalisierungsaspekte untereinander macht die Auseinandersetzung mit einzelnen anspruchsvollen Themen wie dem Datenschutz noch komplexer. Eine Strategie zur Reduktion dieser Komplexität besteht vor allem darin diesen Zusammenhang von vornherein mitzudenken und Insellösungen zu meiden. Data Governance soll daher als organisationsübergreifender Prozess aufgefasst werden.

So muss auch der Datenschutz als ein Teil eines ganzheitlichen Data-Governance-Prozesses begriffen und Datenschutzanforderungen im Zusammenhang mit Aspekten wie Datenqualität, Metadatenmanagement oder Rollenkonzepten von vornherein mitgedacht werden. Gerade weil der Datenschutz viele Aspekte – von der Datenbankarchitektur bis hin zur Datenethik – berührt sind die Datenschutzverantwortlichen als Digitallotsen zu verstehen, die in einen umfassenden, organisationsübergreifenden Data-Governance-Prozess einzubinden sind. Nicht zuletzt durch ganzheitliche und strukturierte Data Governance wird zugleich die Data Literacy der Mitarbeiter:innen gesteigert und eine Datenkultur in den Organisationen aufgebaut.

### Über den Autor

**Dr. Nikolai Horn**
ist Projektkoordinator Data Governance beim unabhängigen Think Tank iRights.Lab. Nach seinem Studium der Philosophie arbeitete er am Institut für Öffentliches Recht der Universität Bonn (Lehrstuhl Prof. Dr. Dr. Udo Di Fabio) und promovierte zum Grundrecht der Gewissensfreiheit. Danach war er bei der Stiftung Datenschutz und beim IT-Beratungshaus Capgemini. Horn ist ehrenamtlich Leiter der AG-Ethik der Initiative D21.

▶ https://irights-lab.de

# RECHTSANWALT UND DATENSCHUTZBEAUFTRAGTER - GENERALIST ODER SPEZIALIST?

Dr. Carlo Piltz

*Welche Voraussetzungen muss ein Datenschutzbeauftragter erfüllen, um seinen gesetzlichen Aufgaben nach DSGVO und BDSG nachkommen zu können? Ist es gar zwingend erforderlich, dass nur Volljuristen als Datenschutzbeauftragte tätig werden können? Und wie interpretieren Behörden und Gerichte die fachlichen und persönlichen Anforderungen an den Datenschutzbeauftragten? Der nachfolgende Beitrag soll hierzu einen kurzen Überblick geben.*

## A. Einleitung

Die belgische Datenschutzbehörde (APD/GBA) verhängte am 13. November 2020 gegen ein Unternehmen ein Bußgeld in Höhe von 1.500 Euro wegen des Verstoßes gegen mehrere grundlegende Pflichten der DSGVO.[1] Unter anderem verstieß das Unternehmen gegen seine Verpflichtung die Einstellung des Datenschutzbeauftragten[2] (DSB) ausreichend anhand der von der DSGVO vorausgesetzten Qualifikationen zu begründen. Gemäß Art. 37 Abs. 5 DSGVO wird der DSB unter anderem auf der Grundlage seines Fachwissens im Datenschutzrecht und in der Datenschutzpraxis benannt. Das Unternehmen ist seiner Verpflichtung jedoch nicht nachgekommen, indem es lediglich eine allgemeine Ausschreibung für einen DSB veröffentlichte, ohne nähere Anforderungen an die Qualifikation zu stellen. Anhand dieser Ausschreibung konnte das Unternehmen die konkret notwendigen Anforderungen an den DSB zumindest nicht ausreichend darlegen.

## B. Welche konkreten Anforderungen bestehen für einen Datenschutzbeauftragten?

Nach Art. 37 Abs. 5 DSGVO wird der DSB auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Art. 39 genannten Aufgaben. Die DSGVO-Anforderungen an die fachliche Qualifikationen sind mithin (mindestens) zweigeteilt: Fachwissen auf dem Gebiet des Datenschutzrechts und Fachwissen auf dem Gebiet der Datenschutzpraxis.

Daneben fordert die DSGVO auch, dass der DSB die „Fähigkeit" besitzt seine gesetzlichen Aufgaben zu erfüllen. Diese Anforderung ist weniger fachspezifisch geprägt, sondern stark von der Person des DSB beeinflusst.

### 1. Fachliche Qualifikation

Nach Ansicht des Europäischen Datenschutzausschusses (EDSA) muss der DSB über Erfah-

[1] Englische Zusammenfassung der Entscheidung bei gdprhub.eu, abrufbar unter: https://gdprhub.eu/index.php?title=APD/GBA_-_73/2020.

[2] Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

rung sowohl im einzelstaatlichen als auch im europäischen Datenschutzrecht und in der diesbezüglichen Praxis sowie über ein umfassendes Verständnis der DSGVO verfügen.[3] Die europäischen Behörden verlangen daher sicher zu einem gewissen Maß eher einen Spezialisten als einen Generalisten. Jedoch ist auch zu beachten, dass innerhalb des Datenschutzrechts noch einmal thematische Bereich existieren, die zu einer weiteren Spezialisierung führen können.

Beispielweise im Gesundheitsbereich: Betrachtet man das Recht als Ganzes und das Datenschutzrecht als ein Spezialgebiet ist aber sicher davon auszugehen, dass der DSB nach Behördenansicht eher ein Spezialist sein muss als ein Generalist. Die Tätigkeit als DSB „mal eben so nebenher" zu erledigen dürfte die Anforderungen der DSGVO nicht erfüllen.

Wie oben beschrieben sind aber nicht allein rechtliche Aspekte von Bedeutung. Auch sollte der DSB über ein gutes Verständnis der durchgeführten Datenverarbeitungsvorgänge, der betreffenden Informationssysteme sowie der Datensicherheits- und Datenschutzerfordernisse verfügen.[4]

Das verlangte Fachwissen ist gesetzlich (wohl bewusst) nicht genau umrissen, muss jedoch mit der Sensibilität, der Komplexität und der Menge der Daten, die eine Einrichtung verarbeitet, im Einklang stehen.[5] Das Fachwissen ist also zu einem gewissen Grad auch kontextbezogen zu ermitteln. Beispiel: Wenn eine Datenverarbeitungstätigkeit besonders komplex ist oder in großem Umfang sensible Informationen betrifft, bedarf der DSB unter Umständen eines höheren Maßes an Fachkompetenz und Unterstützung als bei weniger sensiblen Verarbeitungen.

### 2. Persönliche Voraussetzungen

Der Begriff der „Fähigkeit" zur Erfüllung der dem DSB obliegenden Aufgaben ist nach Ansicht des EDSA im Sinne sowohl seiner persönlichen Eigenschaften und Kenntnisse als auch seiner Position innerhalb der Organisation zu verstehen.[6] Auch hinsichtlich dieses Merkmals scheinen die Behörden also eher von einem Spezialisten auszugehen, der Verarbeitungsvorgänge, Abläufe und die IT-Struktur in der datenverarbeitenden Stelle gut kennen muss.

Zu den persönlichen Eigenschaften zählt der EDSA beispielsweise Integrität und ein ausgeprägtes Berufsethos. Dem DSB kommt eine zentrale Rolle im Unternehmen dabei zu die Verbreitung einer Datenschutzkultur innerhalb der Einrichtung zu fördern und zur Umsetzung wesentlicher Bestandteile der DSGVO beizutragen. Hierfür muss er persönlich geeignet sein. Rein praktisch verlangt also die DSGVO, dass der DSB auch die menschlichen Fähigkeiten besitzt seine Empfehlungen intern verständlich zu adressieren und den Datenschutz in die datenverarbeitende Stelle zu bringen.

Zu den persönlichen Voraussetzungen des DSB gehört außerdem seine Zuverlässigkeit (im alten BDSG noch ausdrücklich in § 4f Abs. 2 BDSG aF erwähnt). Dieses Merkmal wird in Art. 37 Abs. 5 DSGVO zwar nicht explizit genannt, ist aber wohl in der erwähnten „Fähigkeit zur Erfüllung der Aufgaben" enthalten. Die für die Zuverlässigkeit erforderliche persönliche Integrität ist eine wichtige Voraussetzung, damit der Beauftragte seine Unabhängigkeit behaupten und gleichzeitig neutral gegenüber unterschiedlichen Interessenlagen sein kann. Diese Zuverlässigkeit kann insbesondere in Fällen der Interessenkollision in Frage stehen oder wenn der DSB im Rahmen der Ausübung seiner Aufgaben bewusst oder grob fahrlässig rechtswidrig handelt.

### 3. Anforderungen aus der Rechtsprechung

Einige interessante Aussagen zu den Anforderungen an die Person des DSB hat im Jahr 2020 das LAG Mecklenburg-Vorpommern (Urt. v. 25. Februar 2020, 5 Sa 108/19) getroffen. Zu beachten ist, dass dieses Urteil noch zum alten Landesdatenschutzgesetz erging. Die Erwägungen des LAG lassen sich jedoch auch auf die Anforderungen der DSGVO übertragen. Das LAG war mit der Frage befasst, ob eine Person die Anforderungen an die Benennung als DSB erfüllte. Das Gericht unterschied im Rahmen seiner Begründung ausdrücklich zwischen der erforderlichen Sachkunde und der erforderlichen Zuverlässigkeit. Beide Merkmale lassen sich mit der oben erwähnte fachlichen Qualifikation und den persönlichen Eigenschaften vergleichen. Zunächst macht das LAG deutlich, dass das damalige Gesetz die Tätigkeit des DSB nicht an eine bestimmte Ausbildung oder näher bezeichnete Fachkenntnisse knüpft.

[3] WP243, S. 13.
[4] WP243, S. 13.
[5] WP243, S. 13.
[6] WP243, S. 13.

Welche Sachkunde hierfür erforderlich ist, richtet sich dem LAG zufolge insbesondere nach der Größe der zu betreuenden Organisationseinheit, dem Umfang der anfallenden Datenverarbeitungsvorgänge, den eingesetzten IT-Verfahren und dem Typus der anfallenden Daten.

Praxisrelevant ist die Feststellung des LAG, dass nicht erforderlich ist, dass der DSB alle Fähigkeiten selbst in eigener Person vereint. Es ist durchaus möglich, dass der DSB internes oder externes Fachwissen für sich nutzt und bei seiner Aufgabenerfüllung verwendet.

### 4. Zwischenergebnis

Die DSGVO stellt klar auf ein rechtliches Fachwissen des DSB ab. Zudem muss er nach Ansicht der Behörden in Bezug auf die Datenschutzpraxis und die jeweiligen Gegebenheiten in der datenverarbeitenden Stelle genaue Kenntnisse der Prozesse und Datenverarbeitungen haben. Im allgemeinen Vergleich zu anderen Rechtsgebieten verlangt die DSGVO daher wohl tatsächlich den Spezialisten. Jedoch kann es für die Tätigkeit als DSB durchaus genügen besonderes Wissen im Datenschutzrecht allgemein zu haben. Nicht jeder DSB muss Spezialist für den Datenschutz in Krankenhäusern sein. Das Niveau des Fachwissens ist mithin auch immer von dem Umständen abhängig, in denen der DSB tätig ist.

## C. Rechtsanwalt als Datenschutzbeauftragter – muss das, geht das?

Sowohl nach Ansicht des oben zitierten LAG als auch nach Ansicht des EDSA ist für die Tätigkeit als DSB nicht zwingend erforderlich, dass eine Ausbildung zum (Voll)Juristen durchlaufen wurde. Andererseits ist natürlich auch nicht ausgeschlossen, dass Volljuristen als DSB tätig werden.

Erst kürzlich entschied der Anwaltsgerichtshoff („AGH") Hamm (Urt. v. 12. März 2021, 1 AGH 9/19), dass es bei der Tätigkeit des DSB nicht unwesentlich um die Anwendung der datenschutzrechtlichen Vorgaben sowie die Überwachung der Einhaltung der Vorgaben geht. Daher geht der AGH (mit dem BGH, Urt. v. 15. Oktober 2018, AnwZ (Brfg) 20/18) davon aus, dass die Tätigkeit als DSB, je nach den Umständen des Einzelfalls, die Merkmale des § 46 Abs. 3 Bundesrechtsanwaltsordnung (BRAO) erfüllen und hiervon geprägt sein, also sich als anwaltliche Tätigkeit darstellen kann.

Zudem geht der AGH noch weiter und entschied, dass es sich bei der Tätigkeit als DSB zumindest um eine Rechtsdienstleistungstätigkeit im Sinne des § 2 RDG handelt. Die von einem DSB i.S.v. Art. 39 DSGVO erbrachten Rechtsdienstleistungen sind nach Ansicht des AGH gesetzlich erlaubt. Der DSB muss also gerade kein Volljurist oder Rechtsanwalt sein. Ausgeschlossen hat dies der AGH aber auch nicht. Können also (auch weiterhin) Rechtsanwälte als (externe) Datenschutzbeauftragte agieren?[7] Das oben zitierte Urteil des BGH ist diesbezüglich meines Erachtens klar. Der Kern und der Schwerpunkt der Tätigkeit eines Datenschutzbeauftragten liegen grundsätzlich in der Auslegung und Anwendung der datenschutzrechtlichen Vorgaben sowie in der Überwachung der Einhaltung dieser Vorgaben.

Daher, so der BGH im konkreten Fall, habe auch die Tätigkeit als DSB ihren Kern und Schwerpunkt eindeutig auf der rechtlichen Ebene und es waren dort die Merkmale der „anwaltlichen Tätigkeit" nach § 46 Abs. 3 Nr. 1 bis 4 BRAO erfüllt. Gegen die Möglichkeit, dass Anwälte als DSB tätig werden, spricht auch nicht der Einwand, dass der Mandant in diesem Fall nicht Herr des dem Anwalt erteilten Auftrags wäre, sondern dessen Aufsicht und Kontrolle unterläge.[8]

Denn der Mandant (im dortigen Fall der Arbeitgeber) betraut den Anwalt als DSB gerade bewusst und in Kenntnis der Vorgaben des Art. 39 DSGVO mit diesen Aufgaben und diese Aufgabe dient insbesondere auch den Interessen des Mandanten. Es widerspricht nach Ansicht des BGH nicht anwaltlichen Grundsätzen, eine Aufsichtsfunktion (wie jene des DSB) auszuüben. Denn der Mandant selbst betraut im Rahmen seiner Verantwortung für die Einhaltung des Datenschutzes den Anwalt mit der Aufgabe des DSB.[9]

Aber: Nur weil Anwälte als DSB tätig werden können, bedeutet dies nicht, dass jeder Anwalt per se geeignet ist, diese Rolle zu übernehmen. Die Anforderungen der DSGVO an die Fähigkeiten und persönliche Voraussetzungen des DSB gelten unabhängig davon, ob jemand eine juristische Ausbildung durchlaufen hat oder nicht. Auch Rechtsanwälte müssen sich daher an den Vorgaben des Art. 37 Abs. 5 DSGVO messen lassen.

[7] Vgl. zu rein steuerlichen Aspekten: BFH, Urt. v. 14. Januar 2020, VIII R 27/17; der BFH trennt ausdrücklich zwischen der berufsrechtlichen Ebene (BGH) und der steuerlichen Qualifizierung.

[8] BGH, Urt. v. 15.10.2018 - AnwZ (Brfg) 20/18, Rz. 89.

[9] Vgl. BGH, Urt. v. 15.10.2018 - AnwZ (Brfg) 20/18, Rz. 101.

## D. Ausblick

Die DSGVO und die Aufsichtsbehörden sehen den DSB als Spezialisten auf dem Gebiet des Datenschutzrechts, zumindest im direkten Vergleich zu anderen Rechtsgebieten. Zu beachten ist jedoch, dass sich die Tiefe des erforderlichen Fachwissen durchaus unterscheiden kann. Es kommt stets darauf an, in welcher Umgebung und für welche Art von Organisation der DSB tätig ist und welche Verarbeitungen dort durchgeführt werden. Auch Rechtsanwälte können als DSB tätig sein. Jedoch erfüllen sie allein mit der Zulassung zur Rechtsanwaltschaft noch nicht die gesetzlichen Anforderungen an den DSB.


Über den Autor

**Dr. Carlo Piltz**

ist Rechtsanwal bei Piltz Legal, Berlin mit Schwerpunkt Datenschutzrecht.

▶ https://www.piltz.legal/

Piltz Legal

# DIE PRÜFAUFGABEN DES DATENSCHUTZBEAUFTRAGTEN NACH DSGVO

## Reicht eine Abarbeitung von Checklisten aus?

Christian Nawroth, Patrick Grihn

Mit Einführung der Datenschutz-Grundverordnung (DSGVO) hat sich das Anforderungsprofil an Datenschutzbeauftragte (DSB) und den für die Verarbeitung von personenbezogenen Daten Verantwortlichen verändert. Gemäß Artikel 39 „obliegen dem Datenschutzbeauftragten…

- Unterrichtung und Beratung des Verantwortlichen, Auftragsverarbeiter und der Beschäftigten…
- Überwachung der Einhaltung dieser Verordnung…
- Überprüfung der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten, einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und der Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter,
- Beratung … im Zusammenhang mit der Datenschutz-Folgeabschätzung und Überwachung ihrer Durchführung…
- Zusammenarbeit mit den Aufsichtsbehörden…“

Außerdem wird dem Datenschutzbeauftragten die Pflicht zur risikoorientierten Tätigkeit auferlegt.

Im Gegensatz dazu hat der Verantwortliche nach der DSGVO sicherzustellen, dass die Einhaltung der Datenschutz-Grundverordnung gewährleistet ist, und er muss dies auch nachweisen können. Darüber hinaus hat der Verantwortliche diese Sicherstellung zu kontrollieren. Wie eingangs schon erwähnt, berät der Datenschutzbeauftragte den Verantwortlichen bei all diesen Tätigkeiten, sofern der Verantwortliche einen solchen benannt hat.

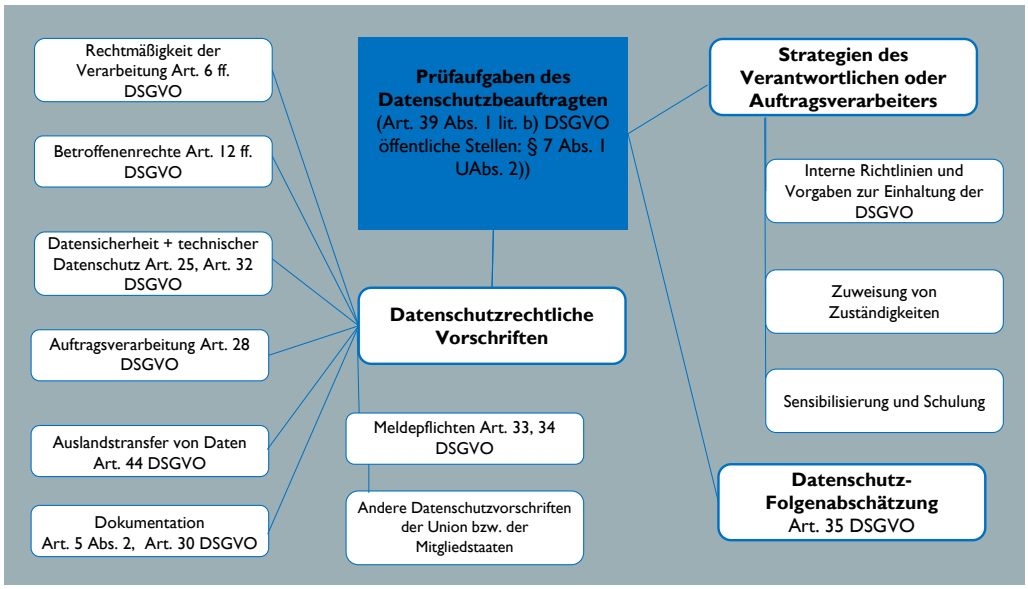
Nachfolgend wollen wir uns diese Anforderungen aus der DSGVO näher ansehen und aufzeigen, welche Auswirkungen diese Anforderungen auf die Arbeit des Datenschutzbeauftragten haben, insbesondere auf Kontrollen und Überprüfungen. Darüber hinaus wollen wir erste Hilfestellungen geben, welche Möglichkeiten sich dadurch auch für den DSB ergeben können.

### Prüfaufgaben DSB - Regelmäßige Kontrollen

Für Datenschutzbeauftragte ergeben sich eine Reihe von Prüfaufgaben auf der Basis von gesetzlichen Anforderungen. Diese ergeben sich vor allem aus Art. 39 Abs. 1 lit. b. DSGVO und § 7 Abs. 1 Nr. 2 BDSG.

Zudem berät der Datenschutzbeauftragte den Verantwortlichen, die Auftragsverarbeiter und die Beschäftigten (Art. 39 Abs. 1 lit. a). Um dieser Beratungsverpflichtung nachkommen zu können ist es wichtig zu wissen, dass dem Verantwortlichen durch die DSGVO zusätzliche Prüfpflichten auferlegt werden. Diese ergeben sich aus den Grundsätzen für die Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 lit. a.-f.) und der Nachweispflicht, für deren Einhaltung diese auch nachzuweisen sind (Art. 5 Abs. 2 und Art. 24 Abs. 1). Außerdem wird dem Verantwortlichen die Pflicht auferlegt, Maßnahmen zu ergreifen und diese Maßnahmen „erforderlichenfalls zu überprüfen und zu aktualisieren“ (Art. 24 Abs. 1). Eine weitere Prüfanforderungen stellt der Art. 32 Abs. 1 lit. d an Verantwortliche, die auch für den Auftragsverarbeiter gilt (Art. 28 Abs. 3 lit. c). Es soll „ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“ etabliert werden. Warum sind diese Anforderungen an den Verantwortlichen und Auftragsbearbeiter auch wichtig für den Datenschutzbeauftragten?

Im Erwägungsgrund 97 wird der Datenschutzbeauftragte als eine Person beschrieben, die den Verantwortlichen oder den Auftragsverarbeiter „bei der Überwachung der internen Einhaltung der Bestimmungen dieser Verordnung“ mit seinem „Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzverfahren“ unterstützten soll. Darüber hinaus gibt es noch eine Reihe von weiteren Prüfanforderungen, bei der ein Datenschutzbeauftragter selbst tätig wird oder beratend unterstützt. Wir




Übersicht der Prüfaufgaben des DSB (© AK Prüfaufgaben des BvD)

können festhalten, es gibt neben der generischen Forderung aus Art. 39 die Einhaltung der DSGVO zu überwachen, keine weitere inhaltliche oder operative Anforderung an den DSB. Leider geht die DSGVO oder das Bundesdatenschutzgesetz nicht weiter darauf ein, wie Datenschutzbeauftragte diese doch sehr unspezifisch gehaltenen Prüfanforderungen explizit operativ umsetzen sollen. Wesentlich konkreter wird die DSGVO da schon bei den Verantwortlichen und Auftragsverarbeitern. In den nachfolgenden Artikeln (Art.) und Erwägungsgründen (ErwG) werden teilweise sehr dedizierte Maßnahmen benannt, die eine regelmäßige Überprüfung nach Wirksamkeit der etablierten Prozesse fordern.

- Art. 24 DSGVO – Verantwortung des für die Verarbeitung Verantwortlichen
- Art. 25 DSGVO – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
- Art. 32 DSGVO – Sicherheit der Verarbeitung
- ErwG 76 DSGVO – Risikobewertung
- ErwG 78 DSGVO – Geeignete technische und organisatorische Maßnahmen
- ErwG 79 DSGVO – Zuteilung der Verantwortlichkeiten
- ErwG 83 DSGVO – Sicherheit der Verarbeitung

Nicht zuletzt sei noch erwähnt, dass sich die Etablierung von geeigneten Prüfverfahren auch auf die Bemessung von Bußgeldern auswirkt. Gemäß Art. 83 Abs. 2 lit. d ist der Grad der Verantwortung davon abhängig, welche Maßnahmen gemäß Art. 25 und 32 der Verantwortliche getroffen hat. Hierfür müssen Verarbeiter Nachweise erbringen. Ganz konkret wird gemäß Art. 32 Abs. 1 lit. d ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit gefordert.

So fordert das berufliche Leitbild des BvD e. V., welchem sich seine Mitglieder unterwerfen, dass der Datenschutzbeauftragte regelmäßige Kontrollen durchführt und sich hierbei an die Vorgaben der DSGVO sowie an angrenzende etablierte Managementsysteme hält. Hierbei werden gängige Zyklen wie der PDCA implizit angeführt und auf die o. g. Grundsätze referenziert.

Insbesondere die vielfältigen Aufgaben- und Prüfbereiche des Datenschutzbeauftragen erfordern ein strukturiertes Management der jeweiligen Segmente (vgl. 2.2. Berufliches Leitbild der Datenschutzbeauftragten, 4. Auflage). So werden die offensichtlichen Bereiche ebenso angeführt wie eine strukturierte Kommunikation mit der Aufsichtsbehörde sowie die regelmäßige systematische Überwachung und Verbesserung des Schulungskonzepts.

## Durchführung von Kontrollen – Systemischer Ansatz

Auch wenn in den Gesetzestexten nicht explizit

beschrieben ist, welche spezifischen Prüfaufgaben den Datenschutzbeauftragten auferlegt werden und was im Detail überprüft bzw. kontrolliert werden muss, damit die Anforderungen aus der DSGVO eingehalten werden, lässt sich doch aus der Datenschutz-Grundverordnung ableiten, welche Anforderungen sich an die Überwachungsaufgaben des DSB ergeben, insbesondere auch durch die Aufgaben des Verantwortlichen und des Auftragsverarbeiters, da deren regelmäßige Überprüfungen Teil der Überwachungsaufgabe der Datenschutzbeauftragten sein können.

Zusammenfassend ergeben sich fünf allgemeine Anforderungen an die Prüfaufgaben eines Datenschutzbeauftragten:

**1. Es muss ein Verfahren etabliert werden.** Verfahren bedeutet geregelt, in Verfahrensschritte zerlegbar, nachvollziehbar und hat einen „wiederholbaren Ablauf".[1]

**2. Diese Verfahren müssen regelmäßig durchgeführt werden.** Eine einmalige Überprüfung ist also nicht ausreichend.

**3. Es muss in Form einer Überprüfung stattfinden.** Mit Überprüfung ist gemeint, dass eine Untersuchung/Analyse durchgeführt wird, die prüft, ob Anforderungen erfüllt sind. In diesem Fall, ob die gesetzlichen Anforderungen eingehalten sind.

**4. Es muss die Wirksamkeit der Maßnahmen bewertet und evaluiert werden.** Hierunter ist neben einer vollständigen Umsetzung der Maßnahmen auch deren mittel- und langfristige Auswirkung zu bewerten, da nicht jede Maßnahme sofort Wirkung zeigt. Außerdem muss die Maßnahme bewertet werden. Mit Evaluierung ist eine sach- und fachgerechte Untersuchung/Bewertung gemeint.[2]

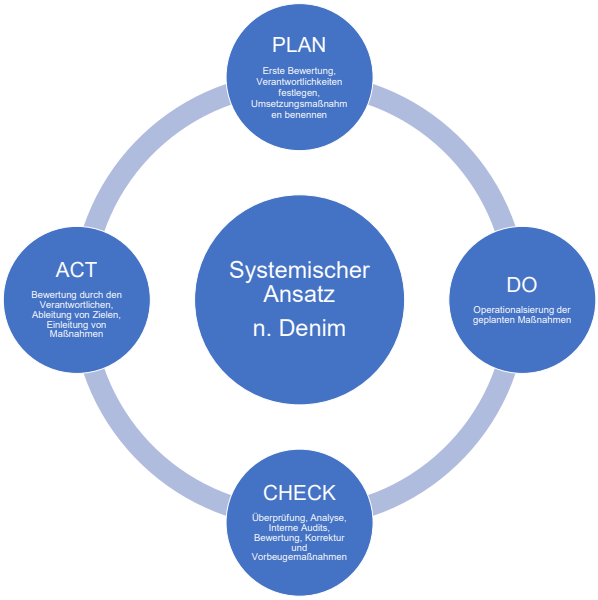
**5. Es muss ein risikobasierter Ansatz adressiert werden.** Bei den Prüfaufgaben ist sicherzustellen, dass die eingerichteten Kontrollen zur Vermeidung von Risiken in allen Bereichen einer Organisation adäquat berücksichtigt und entsprechend etabliert wurden.[3]

Die größte Herausforderung bei der Umsetzung dieser fünf Anforderungen stellt zweifelsfrei der Punkt 3 dar. Bei den zu überprüfenden Anforderungen handelt es sich nicht um eine Norm mit festgelegten Controls, sondern um gesetzliche Anforderungen. Gesetzliche Anforderungen sind aber von Rechtsprechungen abhängig und diese beeinflussen möglicherweise die Validierungsregeln[4]. Das bedeutet für den Datenschutzbeauftragten, dass sich Anforderungen gegebenenfalls im Laufe der Zeit ändern können und er die aktuelle Rechtsprechung im Auge behalten muss.

Generell ergeben sich unterschiedliche Ansätze, wie man die Einhaltung von Anforderungen überwachen kann. Neben dem klassischen Kontrollieren durch das Beobachten, Messen und Befragen mittels Checkliste, Anforderungskatalog oder Inspektionen und Überprüfungen von Aufzeichnungen, kann man Monitoringsysteme etablieren. Darüber hinaus können Tests und Analysen durchgeführt werden. Letztendlich dienen alle genannten Maßnahmen nur der Überprüfung der Anforderungen. Eine Bewertung der Wirksamkeit der Maßnahmen hat damit noch nicht stattgefunden.

Deshalb kann es für den Datenschutzbeauftragten sehr hilfreich sein sich mit systemischen Ansätzen zu beschäftigen, wie man in einer strukturierten Vorgehensweise Anforderungen validiert und wie man konkret die Wirksamkeit von Maßnahmen überprüft. Denn wenn man die Wirksamkeit von Maßnahmen überprüfen will, wird einem schnell klar, dass es sich nicht um eine einmalige Überprüfung handeln kann. Denn Maßnahmen, Verfahren, Prozesse entwickeln sich weiter. Diese Weiterentwicklung kann positiv, aber auch negativ sein. Es ist nicht ausreichend Prozesse zu etablieren, sondern die etablierten Prozesse müssen gelebt werden!

Auch für den Verantwortlichen und Auftragsverarbeiter stellt sich die Frage nach der Wirksamkeit und damit auch für den DSB als Beratenden.




[1] „Wikipedia: Verfahren", https://de.wikipedia.org/wiki/Verfahren, 07.06.2021

[2] „Wikipedia: Evaluation", https://de.wikipedia.org/wiki/Evaluation, 07.06.2021

[3] ISACA: „Audit and Assurance - How to audit GDPR", 2018, Seite 6.

[4] ISACA: „Audit and Assurance - How to audit GDPR", 2018, Seite 5.

Für eine nachhaltige Etablierung des Datenschutzes wird optimalerweise ein systemischer Ansatz („under control") gewählt. Diese Kombination setzt man mit einem Datenschutz-Managementsystem um. Denn nur mit einem Datenschutz-Managementsystem ist man in der Lage der Einhaltung von gesetzlichen Anforderungen adäquat gerecht zu werden.

Optimalerweise wird der Datenschutz in die vorhandenen Prozesse des Verantwortlichen integriert. Als wirksames Instrument hat sich hier der kontinuierliche Verbesserungsprozess nach Denim etabliert. Dieses Verfahren bildet die Basis für alle Managementsysteme der ISO/IEC-Normen und gewährleistet durch den Ansatz der kontinuierlichen Verbesserung auch eine langfristige Bewertung der Wirksamkeit.

## Systemischer Ansatz nach Denim

Für die Überprüfung von Datenschutzmanagementsystemen (DSMS) ist ebenfalls eine systemische Vorgehensweise zu empfehlen. Für die Untersuchung von Prozessen, Richtlinien, Anforderungen hat sich die Durchführung von Audits als erprobte, praktische Maßnahme etabliert. Nachfolgende Standards der Internationalen Organisation für Normung (ISO), dem globalen Berufsverband für IT-Revisoren, Wirtschaftsprüfer sowie Experten der Informationssicherheit und IT-Governance (ISACA) und dem Institut der Wirtschaftsprüfer in Deutschland (IDW) können als Leitfaden für die Durchführung von Audits dienen. Im Detail geht es um die Standards:

- **ISO 19011** – Leitfaden zur Auditierung von Managementsystemen
- **ISACA – Auditing-Standards – Auditing-Guidelines – Auditing-Procedures & Code of Professional Ethics** General (1000 series) - Performance (1200 series) - Reporting (1400 series)
- **IDW PS 860** – Prüfungsstandard für alle Sonderprüfungen im IT-Umfeld

Alle anderen genannten Standards legen Prinzipien für die Durchführung der Prüfung/Audits fest. Diese Prinzipien sind die Grundlage für die Audits und müssen natürlich vom Auditor eingehalten werden.

| DIN EN ISO 19011 | ISACA-IT-Prüfungsstandard | Prüfungsstandard IDW PS 860 |
|---|---|---|
| • Integrität<br>• Sachliche Darstellung<br>• Angemessene berufliche Sorgfaltspflicht<br>• Vertraulichkeit<br>• Unabhängigkeit<br>• Faktenbasierter Ansatz (Vorgehensweise, die auf Nachweisen beruht)<br>• Risikobasierter Ansatz | • Formale Beauftragung<br>• Unabhängigkeit<br>• Rechtschaffenheit & Vertraulichkeit<br>• Fachkompetenz<br>• Nachweis & Nachvollziehbarkeit<br>• Objektivität & Sorgfalt<br>• Sachliche Darstellung | • Relevanz<br>• Vollständigkeit<br>• Verlässlichkeit<br>• Neutralität<br>• Verständlichkeit<br>Ergänzende berufliche Grundsätze der Wirtschaftsprüfer:<br>• Unabhängigkeit, Unparteilichkeit und Vermeidung der Besorgnis der Befangenheit<br>• Gewissenhaftigkeit einschl. beruflicher Kompetenz und der berufsüblichen Sorgfalt<br>• Verschwiegenheit<br>• Eigenverantwortlichkeit<br>• Berufswürdiges Verhalten, einschließlich Verantwortung gegenüber dem Berufsstand |

## Kriterien der Durchführung von Audits

Darüber hinaus gibt es Kriterien an den Auditor selbst. Zusammenfassend sollten Auditoren, die Datenschutzprüfaufgaben wahrnehmen, befähigt sein, Audits durchzuführen. Kranig/Sachs/Gierschmann nennen in „Datenschutzcompliance nach DS-GVO" zusammenfassend die nachfolgenden Anforderungen:[5]

- Fach- und Methodenwissen besitzen
- Soziale Kompetenz haben
- Von den Auditierten als Kompetenz akzeptiert werden
- Sachliche, zielgerichtete und objektive Arbeitsweise haben
- Standhafte Konfliktfähigkeit haben
- Rechtliche Kenntnisse besitzen
- Kenntnisse in der Informationssicherheit haben
- Tiefgreifende Kenntnisse des technischen Datenschutzes haben
- Bei Cloud-Architekturen ein vertieftes Wissen zum internationalen Datentransfer und cloudspezifischer Bedrohungslagen haben

Als BluePrint für die Durchführung von Audits kann die ISO 19011 gut herangezogen werden. Sie beschreibt und regelt das Thema Audits in Form eines „Leitfadens zur Auditierung von Managementsystemen"[6]. Neben der Steuerung eines Auditprogramms wird die Durchführung von Audits sowie die Kompetenz und Bewertung von Audi-

[5] Kranig, Sachs, Gierschmann: Datenschutz-Compliance nach der DS-GVO, Bundesanzeiger Verlag, 2017, S.148

[6] „ISO 19011", https://de.wikipedia.org/wiki/ISO_19011, 15.06.2021

toren geregelt. Außerdem gibt es im Anhang A eine Anleitung für Auditoren zum Planen und Durchführen von Audits (informativ). Dort wird in 18 Unterkapiteln ausführlich operative Hilfestellung gegeben.[7] Diese Norm kann dem Datenschutzbeauftragten als allgemeine Grundlage dienen, wie er seine Prüfaufgaben organisiert und welche Rahmenparameter er wählt, um seine Audits in einer strukturierten Form ablaufen zu lassen. Da die ISO 19011 ein allgemeiner Standard für die Durchführung von Audits ist, bietet sie dem Datenschutzbeauftragten keine inhaltliche Hilfe an, was die Datenschutz-Grundverordnung und das BDSG in Bezug auf die Einhaltung des Datenschutzes explizit fordert.

Speziell für die Prüfung der Organisation des Datenschutzes hat sich mit „IDW PH 9.860.1 für Prüfungen nach der DSGVO und dem BDSG" ein dediziertes Rahmenwerk etabliert. Hier wird neben dem Umfeld die Aufbauorganisation und die Ablauforganisation auditiert. Im Detail sind das die Bereiche:

- Tätigkeit des DSB
- Risikomanagement
- Rechtmäßigkeit der Verarbeitung
- Verzeichnis der Verarbeitungstätigkeiten
- Privacy by Design / Privacy by Default
- Übermittlung in Drittländer
- Auftragsverarbeitung
- Datenschutzverletzung
- Betroffenenrechte
- Löschmanagement
- Sicherheit der Verarbeitung

Als Alternative dazu kann auch das Audit-Programm der ISACA (GDPR – Audit) hilfreich sein. Es basiert auf Durchführungskontrollen (Implementation Controls) und Erhaltungskontrollen (Maintenance Controls).[8] Im Audit werden 9 Datenschutzcluster (DPP) untersucht.[9]

- DPP1 - Betreiben eines Datenschutz-Management-System
- DPP2 - Erfassen, Identifizieren und Klassifizieren persönlicher Daten
- DPP3 - Umgang mit Datenschutz Risiken
- DPP4 - Umgang mit Datensicherheit
- DPP5 - Lieferketten und Auftragsverarbeiter
- DPP6 - Management von Verstößen und Vorfällen
- DPP7 - Bewusstsein schaffen und aufrechterhalten
- DPP8 - Organisation Datenschutz und DSB
- DPP9 - Betrieb von interne Kontrollen

Auch die gerade verabschiedete DIN EN ISO/IEC 27701:2021 („Deutsche Fassung der Sicherheitstechniken - Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Management von Informationen zum Datenschutz - Anforderungen und Leitlinien (ISO/IEC 27701:2019)) kann hier für den Datenschutzbeauftragten hilfreich sein. Die dort beschriebenen spezifischen Anforderungen an ein Privacy Information Managementsystem (PIMS) stellen eine übersichtliche Ergänzung dar.

## Empfehlung und Fazit

Es zeigt sich, dass nur ein systemischer Ansatz und eine strukturierte Vorgehensweise bei der Überprüfung (Audit) der Einhaltung der Anforderungen aus der DSGVO und des BDSG ausreichend und geeignet sein kann. Hierfür muss ein Verfahren etabliert werden. Dieses Verfahren muss regelmäßig durchgeführt werden. Optimalerweise wird diese Überprüfung als strukturiertes Audit durchgeführt und es wird der risikobasierte Ansatz berücksichtigt. Vor allem aber muss die Wirksamkeit der Maßnahmen bewertet und evaluiert werden. Diese Forderung legt die Messlatte für die Prüfungen durch den Datenschutzbeauftragten und den Verantwortlichen hoch. Dadurch wird auch bei den Prüfaufgaben eine nachhaltige Sicht auf die Verfahren, Prozesse und Maßnahmen des Datenschutz erforderlich. Dies lässt sich mit einer Momentaufnahme mittels Checkliste nicht umsetzen.


### Über die Autoren

**Christian Nawroth**
Seit 1991 als technischer Consultant im Enterprise Umfeld tätig und seit 2002 Inhaber des Beratungsunternehmens SIGU-CONSULT. Außerdem ist er Mitglied des BvD Ausschuss Prüfaufgaben Datenschutzbeauftragter.

**Patrick Grihn**
Als Geschäftsführer der nextindex GmbH & Co. KG betreut er mit seinem Team KMUs in den Bereichen IT-Infrastruktur, IT-Sicherheit und Datenschutz.


### Über den BvD-Ausschuss

Beide Autoren sind Mitglied im Ausschuss Prüfaufgaben Datenschutzbeauftragter des BvD, der einen einheitlichen Prüfkatalog als Arbeitshilfe für den Datenschutzbeauftragten bei Audits erarbeitet.

[7] Beuth-Verlag: „Inhaltsverzeichnis DIN EN ISO 19011:2018-10", https://www.beuth.de/de/norm/din-en-iso-19011/287794262, 15.06.2021

[8] ISACA: „Audit Pogram Narrativ - GDPR Audit Program", 2018, Seite 5.

[9] ISACA Auditcheckliste GDPR_Audit_Program_Enterprise.xlsx

# ISO 19011 ALS GRUNDLAGE FÜR DATENSCHUTZAUDITS

## Der systemische Ansatz

Stephan Rehfeld

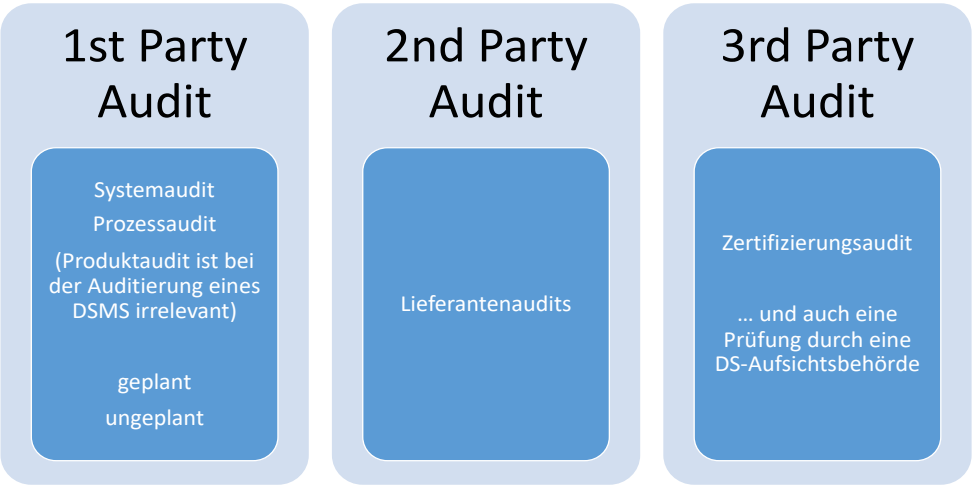
Unter der Ägide der Datenschutz-Grundverordnung (DSGVO) ist eine Aufgabe des Datenschutzbeauftragten die Organisation von Datenschutzaudits. Christian Nawroth und Patrick Grihn haben in ihrem vorangestellten Artikel die gesetzlichen Grundlagen des Datenschutzbeauftragten, des Verantwortlichen und des Auftragsverarbeiters für die Organisation und die Durchführung von Datenschutzaudits herausgearbeitet und begründet, warum nur ein systemischer Ansatz für die Durchführung von DSGVO-konformen Datenschutzaudits geeignet sein kann.

Die Autoren weisen in ihrem Artikel darauf hin, dass „[…] die Datenschutz-Grundverordnung oder das Bundesdatenschutzgesetz nicht weiter darauf [eingehen], wie Datenschutzbeauftragte diese doch sehr unspezifisch gehaltenen Prüfanforderungen explizit operativ umsetzen sollen."

Die Autoren haben herausgearbeitet, dass ein systemischer Ansatz zur Erfüllung der Datenschutzanforderungen der DSGVO an Datenschutzaudits fünf Anforderungen erfüllen muss:

- Es muss ein Verfahren etabliert werden.
- Dieses Verfahren muss regelmäßig durchgeführt werden.
- Es muss in Form einer Überprüfung stattfinden.
- Es muss die Wirksamkeit der Maßnahmen bewertet und evaluiert werden.
- Es muss ein risikobasierter Ansatz adressiert werden.

Die Autoren ziehen das Fazit „[…], dass nur ein systemischer Ansatz und eine strukturierte Vorgehensweise bei der Überprüfung (Audit) der Einhaltung der Anforderungen aus der DSGVO und des BDSG ausreichend und geeignet sein kann." In diesem Artikel soll untersucht werden, inwieweit mit der ISO 19011:2018[1] ein DSGVO-konformes Vorgehen beschrieben wird, dass den Datenschutzbeauftragten, Verantwortlichen und/oder Auftragsverarbeiter dabei unterstützen kann Datenschutzaudits so zu planen und durchzuführen, dass die Anforderungen an einen systemischen Auditansatz erfüllt werden können.




[1] Im Weiteren wird auf die nationale Norm DIN EN ISO 19011:2018-10 Leitfaden zur Auditierung von Managementsystemen (ISO 19011:2018) Bezug genommen, wenn von der ISO 19011:2018 berichtet wird.

## Audittypen

In der Praxis können verschiedene Audittypen unterschieden werden:

- Compliance-Audits
- Systemaudits
- Prozessaudits
- Produktaudits

Im Folgenden wird nur auf System- und Prozessaudits weiter eingegangen.

Als **Erstparteienaudit (1st Party Audit)** werden interne Audits bezeichnet. Eigene Mitarbeiter oder Dienstleister überprüfen für den Verantwortlichen die eigene Organisation nach Kriterien, die der Verantwortliche vorgegeben hat. Die Ergebnisse dienen zu eigenen Zwecken, wie der Erfüllung der organisationseigenen Nachweispflichten nach DSGVO.

Solche Erstparteienaudits können geplant oder ungeplant erfolgen. Im Regelfall erfolgen die internen Audits geplant und werden lang- oder mittelfristig im Rahmen eines Auditprogramms terminiert und mit den zu auditierenden Abteilungen terminiert. Ungeplante Audits können zum Beispiel durch Beschwerden oder Datenschutzvorfälle ausgelöst werden. Hier kann es erforderlich sein, dass kurzfristig überprüft wird, ob in Geschäftsprozessen die Datenschutzanforderungen eingehalten werden. Ungeplante Audits sollten der Ausnahmefall sein.

Weiterhin kann zwischen System- und Prozessaudits unterschieden werden. Bei einem Systemaudit wird das gesamte System auf sein generelles Funktionieren überprüft. Dies ist die Vogelperspektive auf ein Datenschutz-Managementsystem (DSMS). Bei einem Prozessaudit hingegen werden die zu untersuchenden Geschäftsprozesse auf Konformität untersucht. In der Praxis ist der Übergang von einem Systemaudit zu einem Prozessaudit fließend. Bei der erstmaligen Aufnahme eines Auditprogramms in einer Organisation wird ein Systemaudit im Vordergrund stehen, da meist erstmal die Frage geklärt werden soll, ob der betriebliche Datenschutz prinzipiell „funktioniert". Mit einer größeren Anzahl an durchgeführten Audits wird die Detailtiefe in den Vordergrund treten und die Prozessaudits werden wichtiger.

**Als Zweitparteienaudit (2nd Party Audits)** werden Lieferantenaudits bezeichnet. Bei Lieferantenaudits werden im Datenschutz Auftragsverarbeiter durch den Auftraggeber auditiert. Die Audits können durch eigenes Personal des Verantwortlichen durchgeführt werden oder durch beauftragte Dritte. In der DSGVO sind Lieferantenaudits in Art. 28. Abs. 3 lit. h DSGVO explizit vorgesehen.

**Als Drittparteienaudits (3rd Party Audits)** werden Zertifizierungsaudits bezeichnet. Hier beauftragt der Verantwortlichen einen Zertifizierer damit, ein Audit durchzuführen. Als Auditkriterium dient meistens ein Standard. Anders ist dies bei einer sogenannten Artikel-42-Zertifizierung. Hier wird gegen die DSGVO geprüft. Auch eine anlassfreie Prüfung durch eine Datenschutz-Aufsichtsbehörde kann systematisch als ein 3rd Party Audit aufgefasst werden.

Die ISO 19011:2018 ist ein Leitfaden, in dem allgemein die Auditierung von Managementsystemen beschrieben wird. Das Vorgehensmodell der ISO 19011:2018 kann bei den hier beschriebenen 1st, 2nd und 3rd Party Audits angewendet werden. In der ISO 19011:2018 wird nicht auf Produktaudits eingegangen und sie kann auf beliebige Themen von Managementsystemen angewendet werden, also etwa für Datenschutzaudits, aber auch Audits des Informationssicherheitsmanagements, des Qualitätsmanagements oder des Umweltmanagements. Die Kombination von Audits aus mehreren Management-Normen ist mit der ISO 19011:2018 möglich (auch als integrierte Audits bezeichnet) und durchaus gewollt.

## Auditprinzipien

Die Auditprinzipien der ISO 19011:2018 sind die Grundlage der Arbeit der Auditoren bei der Prüfung eines (Datenschutz-) Managementsystems. Beim Auditieren müssen Auditoren die Auditprinzipien einhalten, damit unterschiedliche Auditoren zu identischen oder zumindest ähnlichen Auditergebnissen kommen (würden).
Ferner müssen die Auditprinzipien eingehalten werden, um bei den Personen in der zu auditierenden Organisation ausreichend Vertrauen zu erzeugen, um eine freie und wahrheitsgemäße Beantwortung zu ermöglichen (oder dieser nicht entgegenzuwirken).

In der ISO 19011:2018 werden die folgenden Auditprinzipien genannt:[2]

- Integrität
- sachliche Darstellung
- angemessene beruflich Sorgfalt
- Vertraulichkeit hinsichtlich der Sicherheit von Informationen
- Unabhängigkeit
- faktengestützter Ansatz
- risikobasierter Ansatz

Obwohl alle Auditprinzipien für ein erfolgreiches Audit wichtig sind, sollen drei Prinzipien genauer vorgestellt werden.

Mit dem **faktengestützten Ansatz** ist gemeint, dass Auditschlussfolgerungen auf nachvollziehbaren Fakten (sogenannten Nachweisen) gestützt werden und auf einer angemessenen Stichprobe basieren müssen. In einem engen Zusammenhang mit dem faktengestützten Ansatz steht die **sachliche Darstellung** eines Auditergebnisses.

Die Darstellung von Feststellungen und Auditschlussfolgerungen muss wahrheitsgemäß erfolgen. Sollte über eine Feststellung oder eine Auditschlussfolgerung zwischen der auditierten Organisation und dem Auditor Uneinigkeit bestehen, so muss der Auditor in seinem Bericht auch darüber objektiv und wahrheitsgemäß berichten.

Unter dem **risikobasierten Ansatz** fordert der Standard schwerpunktmäßig die Themen zu auditieren, die einen maßgeblichen Einfluss auf die Ziele des Managementsystems haben. Für den Auditor ergeben sich also die Auditschwerpunkte aus dem Managementsystem selbst.

## Auditprogramm

Ein Audit ist in der ISO 19011:2018 keine Tätigkeit, die zufällig passiert. Stattdessen muss **der Auditauftraggeber** einen Auftrag zur Erstellung eines Auditprogramms an den **Auditprogrammleiter** geben. Der Auftraggeber ist typischerweise das Top-Management der zu auditierenden Organisation und der Auditprogrammleiter ist regelmäßig der Managementsystembeauftragte. Dies wird in der Praxis häufig der Datenschutzbeauftragte sein. Ob hier Konflikte mit der gesetzlich definierten Rolle des Datenschutzbeauftragten entstehen können, muss in Zukunft geklärt werden.

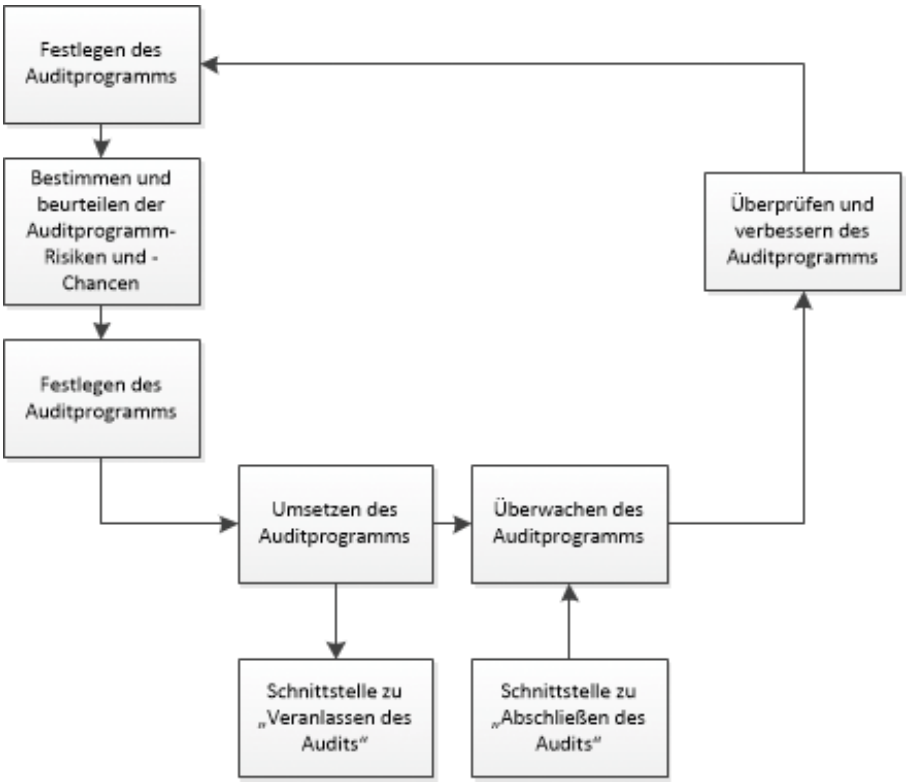



Abbildung 1: Prozessablauf für die Steuerung eines Auditprogramms (Auszug), DIN EN ISO 19011:2018-10, S. 23

Ein **Auditprogramm** ist die Planung und Durchführung von Audittätigkeiten für einen definierten Zeitraum. Der Umfang eines (Datenschutz-) Auditprogramms hängt von verschiedenen Faktoren ab, wie der Kritikalität der zu verarbeitenden personenbezogenen Daten oder der Größe der zu auditierenden Organisation.

In der ISO 19011:2018 wird der folgende Prozess zur Steuerung eines Auditprogramms vorgeschlagen: Bei der Festlegung eines Auditprogramms sollten folgende Informationen erfasst werden (Auszug):[3]

- Ziele für das Auditprogramm
- Risiken und Chancen in Verbindung mit dem Auditprogramm

[2] DIN EN ISO 19011:2018-10, S. 18 ff
[3] DIN EN ISO 19011:2018-10, S. 22

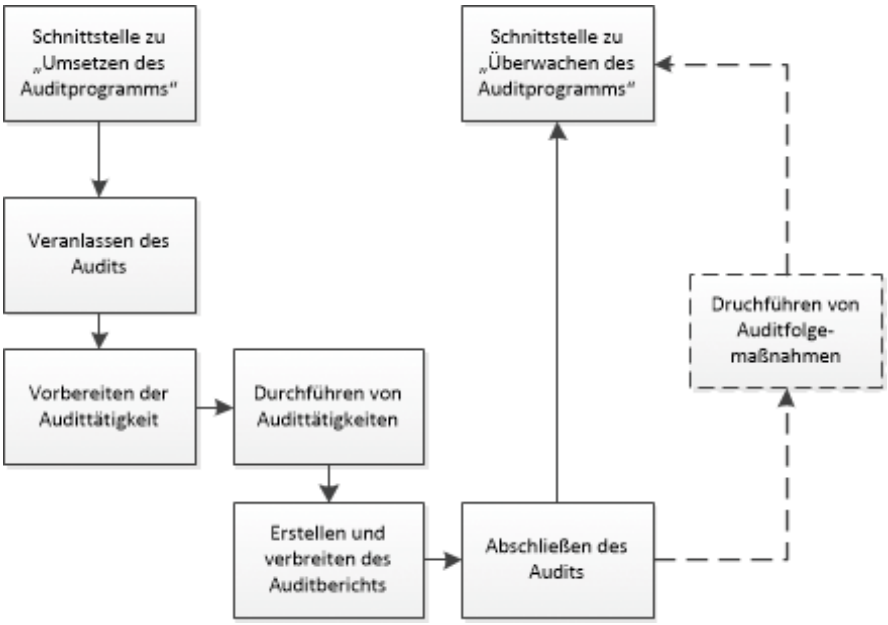



Abbildung 2: Prozessablauf für die Steuerung eines Auditprogramms (Auszug), DIN EN ISO 19011:2018-10, S. 23

- Umfang (Ausmaß, Grenzen, Standorte) jedes Audits des Auditprogramms
- Zeitplan (Anzahl, Dauer, Häufigkeit) der Audits

Hierbei sollte ein besonderes Augenmerk darauf gerichtet werden, dass die Ziele des Auditprogramms und die Auditkriterien klar definiert sind, damit bei den interessierten Parteien keine Enttäuschung über das Ergebnis des Auditprogramms entstehen.

Die Planung, Durchführung, Überwachung und Verbesserung eines Auditprogramms nach ISO 19011:2018 wird in dem Standard sehr ausführlich beschrieben, kann hier aber nicht weiter ausgeführt werden.

## Auditdurchführung

Auch die Durchführung eines Audits, die Inhalte eines Auditberichts bis hin zur Durchführung von Auditfolgemaßnahmen werden in der ISO 19011:2018 detailliert beschrieben.

Der leitende Auditor hat die Aufgabe mit dem zu auditierenden Bereich der Organisation Kontakt aufzunehmen und das Audit zu planen. Bei der Vorbereitung der Audittätigkeit wird der Auditplan auf Grundlage des Auditprogramms und der vorab geprüften Dokumentation von dem/den Auditor(en) erstellt. Anschließend wird das eigentliche Audit durchgeführt. Während des Audits sammeln die Auditoren objektive Nachweise, um die Konformität oder die Nichtkonformität des auditierten Bereichs mit den Auditzielen feststellen zu können. Die Auditfeststellungen werden mit dem auditierten Bereich am Ende das Audits besprochen und in einem Auditbericht dokumentiert. Bei Nichtkonformität, also Abweichungen von den Auditzielen oder systematischen Mängeln, werden mit dem auditierten Bereich Korrekturmaßnahmen vereinbart. Diese Korrekturmaßnahmen müssen nach der Umsetzung auf ihre Wirksamkeit überprüft werden. Der Auditbericht wird dem Auditprogrammleiter und auch dem Top-Management zur Auswertung übermittelt. In kleineren Organisationen wird die Aufgabe des Auditprogrammleiters und des Auditors dem Datenschutzbeauftragten zufallen.

## Fazit

Die vorstehenden Ausführungen sollen zur Beurteilung dienen, ob die ISO 19011:2018 ein Standard ist, der einen Datenschutzbeauftragten, Verantwortlichen oder Auftragsverarbeiter bei der Erfüllung seiner gesetzlichen Datenschutz-Auditverpflichtung nach DSGVO unterstützt und einen systemischen Ansatz verfolgt. Nach Nawroth/Grihn müssen dazu die folgenden fünf Anforderungen erfüllt werden:

- Es muss ein Verfahren (Prozess) etabliert werden. Der Standard ISO 19011:2018 beschreibt einen Prozess zur Planung, Durchführung, Überwachung und Verbesserung eines Auditprogramms, dass alle Audits innerhalb eines definierten Zeitraums umfasst. Auch die Auditdurchführung wird in einem Prozess beschrieben.
- Diese Verfahren (Prozesse) müssen regelmäßig durchgeführt werden. Ein Auditprogramm nach ISO 19011:2018 basiert auf dem PDCA-Zyklus. Somit ist die Planung, Durchführung, Überwachung und Verbesserung als zyklischer Prozess angelegt und Audits müssen von der zu auditierenden Organisation regelmäßig durchgeführt werden.
- Es muss in Form einer Überprüfung stattfinden. Die ISO 19011:2018 ist bei der Definition der Auditziele und der Auditkriterien offen. Wenn die zu auditierende Organisation festlegt, dass ein Auditziel die Feststellung der Datenschutz-Compliance im Stichprobenumfang ist und als Auditkriterien die anzuwendenden Datenschutzgesetze benannt werden (z.B. DSGVO und BDSG-neu), wird diese Anforderung von Nawroth/Grihn durch die ISO 19011:2018 erfüllt.

- Es muss die Wirksamkeit der Maßnahmen bewertet und evaluiert werden. Im Audit ist es Aufgabe der Auditoren nach objektiven Nachweisen für die Konformität oder Nichtkonformität des DSMS zu suchen. Eine Nichtkonformität kann auch eine systematische Verletzung von Anforderungen sein.
- Es muss ein risikobasierter Ansatz adressiert werden. Für Audits nach der ISO 19011:2018 werden Auditprinzipien verbindlich vorgeschrieben. Ein Auditprinzip ist die Berücksichtigung des risikobasierten Ansatzes bei der Planung und Umsetzung des Auditprogramms.

**Fazit:** Die ISO 19011:2018 ist als Rahmenwerk für die Auditierung von Datenschutz-Managementsystemen bzw. der Bewertung der Einhaltung von gesetzlichen Anforderungen für einen Datenschutzbeauftragten oder eine Organisation geeignet, die Forderung nach einem systemischen Ansatz für Datenschutzaudits zu erfüllen.

## Über den Autor

**Dipl.-Ök. Stephan Rehfeld**
ist externer Datenschutzbeauftragter der scope & focus GmbH Hannover und akkreditierter Datenschutzauditor der DQS GmbH. Als stimmberechtigtes Mitglied des AK05 des NIA27 des DIN arbeitet er aktiv an der Erstellung und Überarbeitung von Datenschutz-ISO- und -DIN-Normen mit. Ferner ist er im Leitungskreis des GDD-Erfa-Kreises Hannover engagiert, im AK Datenschutz der Bitkom und in der Fachgruppe Datenschutz von Niedersachsen.Digital e.V.
Stephan Rehfeld ist außerdem BvD-Vorstandsmitglied und Mitglied im Ausschuss Prüfaufgaben Datenschutzbeauftragter des BvD.


# DATENSCHUTZKONFORMES LÖSCHEN BEI DATENSCHUTZ- UND INFORMATIONS-SICHERHEITSVORFÄLLEN

Louisa Rudolph, Dr. Annika Selzer, Dr. Ulrich Pordesch

## Vorschlag einer Löschregel

Informationssicherheits- und Datenschutzvorfälle müssen erkannt, analysiert, bewertet, gemeldet und unter anderem zum Nachweis korrekten Handelns dokumentiert werden. Die Dokumentation enthält meist personenbezogene Daten, fast immer die der Bearbeiter des Vorfalls, aber auch die von Betroffenen oder Dritten. In diesem Beitrag wird erörtert, wann personenbezogene Daten, die im Rahmen einer Dokumentation von Datenschutz- und Sicherheitsvorfällen anfallen, entsprechend der Vorgaben der DSGO zu löschen sind und wie eine Löschregel zur Vorfalldokumentation für einen Löschregelkatalog gebildet werden kann.

## 1. Was sind Datenschutz- und Informationssicherheitsvorfälle und wieso bedarf es eines Vorfallmanagements?[1]

Informationssicherheitsvorfälle können in vielen verschiedenen Formen auftreten, zum Beispiel in Form von technischen Fehlern, Malware-Attacken, Hackerangriffen, Überwachungen des Datenverkehrs, Sabotage gegen die IT-Infrastruktur, unbefugte Datenverschlüsselung oder Datendiebstahl. In vielen Fällen geht es dabei um Betrug, Erpressung, Industrie- oder Wirtschaftsspionage, also die Schädigung der Unternehmen. Vielfach sind jedoch auch Personen und deren Daten das Ziel der Attacken oder sie sind von Attacken und Fehlern mittelbar betroffen. Beispiele hierfür sind der versehentliche Versand von personenbezogenen Informationen an falsche Mail-Adressen bei Beantwortung von Ersuchen betroffener Personen[2], oder das Stehlen von E-Mails und Kontakten, um gezielte Phishing-Attacken gegen Dritte durchzuführen. Ein IT-Sicherheitsvorfall ist in solchen Fällen zugleich auch ein Datenschutzvorfall.[3] Viele Unternehmen und Organisationen sind aufgrund branchenspezifischer Vorgaben verpflichtet, IT-Sicherheitsvorfälle zu melden und geeignete Maßnahmen zur Schadensbegrenzung vorzunehmen. Unternehmen, die solche konkreten Verpflichtungen nicht haben, trifft immer noch die allgemeine Pflicht zum Risikomanagement und damit auch zur Vorfallbehandlung, etwa über das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) oder aufgrund vertraglicher Verpflichtungen, Qualitäts- und Sicherheitszertifizierungen. Bei Datenschutzvorfällen ergeben sich insbesondere aus der DSGVO die folgenden konkreten Verpflichtungen:

- die unverzügliche Meldung von Verletzungen des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt (Art. 33 Abs. 1 DSGVO),
- die unverzügliche Benachrichtigung der betroffenen Personen, sofern die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat (Art. 34 Abs. 1 DSGVO).

Um den Verpflichtungen nachzukommen, müssen Sicherheits- und Datenschutzvorfälle erkannt, analysiert, bewertet und gemeldet werden; es sind die Schadensfolgen zu begrenzen und zu beseitigen und Maßnahmen gegen eine Wiederholung zu ergreifen. Dies erfordert ein Vorfall-Management mit geregelten Zuständigkeiten und Prozessen. Da Informationssicher-

[1] Dieser Beitrag wurde vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt. Der Beitrag gibt die persönliche Meinung der Autorinnen und des Autors wieder und ist keine offizielle Stellungnahme der Fraunhofer Gesellschaft.

[2] Jandt, in: Kühling/ Buchner, DS-GVO BDSG, Art. 4 Abs. 12 DSGVO, Rn. 7.

[3] https://www.verbraucherzentrale.de/wissen/digitale-welt/apps-und-software/emotet-trojaner-beantwortet-empfangene-emails-und-klaut-anhaenge-35502.

heits- und Datenschutzvorfälle vielfach nicht voneinander zu trennen sind, ist dabei ein integriertes einheitliches Management von Datenschutz- und Informationssicherheitsvorfällen sinnvoll.

Ein Datenschutz- und Informationssicherheitsvorfallmanagement beschäftigt sich mit dem Umgang mit Verletzungen des Schutzes personenbezogener Daten (Datenschutz) und von Informationen und IT-Systemen (Informationssicherheit). Eine Verletzung des Schutzes personenbezogener Daten ist eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden (Art. 4 Nr. 12 DSGVO). Während bei Datenschutzvorfällen der für die betroffenen Personen entstehende Schaden im Vordergrund steht, bedeuten Informationssicherheitsvorfälle zumeist einen wirtschaftliche Schaden für das Unternehmen, der durch den unbefugten Zugriff auf Daten wie beispielsweise Patentanmeldungen, abgegebene Angebote oder Rezepturen entstehen kann.[4]

Da Datenschutz- und Informationssicherheitsvorfälle je nach deren Ausprägung unterschiedliche Risiken bergen und unterschiedlich schwere Folgen auslösen können, welche wiederum unterschiedliche Maßnahmen erfordern, obliegt es dem Verantwortlichen nach Kenntnis eines Datenschutz- oder Informationssicherheitsvorfalls eine Risikoeinschätzung vorzunehmen, auf Basis derer Abhilfemaßnahmen zu treffen sind.

## 2. Was wird im Rahmen des Vorfallmanagements dokumentiert?

Voraussetzung dafür, dass Vorfälle analysiert, bewertet und gemeldet werden können und dass Maßnahmen zur Schadensbegrenzung und Strafverfolgung daraus abgeleitet werden können, ist Angaben über eine mögliche Aufklärung des Vorfalls zu erfassen und zu speichern. Dazu zählen E-Mails, Notizen über Gespräche und Analyseergebnisse, Meldezeitpunkte und Melder, Listen betroffener Systeme, geschädigter Personen oder Unternehmen sowie Beweismittel wie gefälschte E-Mails und Protokolldaten. Vorfälle müssen möglichst nach einem standardisierten Verfahren dokumentiert werden.[5]


Neben dem unmittelbaren Zweck den Vorfall selbst bearbeiten zu können erfüllt die Dokumentation viele weitere Zwecke. Sie ist die Grundlage einer eventuellen späteren straf- oder zivilrechtlichen Verfolgung von Schadensverursachern. Sie ermöglicht es bei neuerlichen Vorfällen Parallelen zu erkennen und in einer Nachbearbeitung zu erkennen, ob IT, Regelungen oder Unternehmensprozesse anzupassen sind. Und sie dient nicht zuletzt, vor allem bei den gesetzlich geregelten Meldepflichten, dem Nachweis des korrekten Handelns gegenüber Dritten.

Art. 5 Abs. 2 i.V.m. Art. 24 Abs. 1 DSGVO erlegt dem Verantwortlichen die Pflicht zur Dokumentation von Datenschutzvorfällen auf.[6] Dies soll vor allem die Aufsichtsbehörde zur Kontrolle der Einhaltung rechtlicher Vorgaben befähigen.[7] Wichtig ist hierbei vor allem die Umstände des Vorfalls, der ergriffenen Maßnahmen und des eingetretenen Schadens zu dokumentieren. Insbesondere sollten jegliche vorgenommene Abwägungen Teil der Dokumentation sein.[8] Kurz gesagt, es muss der Nachweis erfolgen, dass im Rahmen des Vorfallmanagements alles Erforderliche getan wurde, um den Schutz der betroffenen Personen und der relevanten Daten zu erreichen.

[4] Hanschke, Informationssicherheit und Datenschutz systematisch und nachhaltig gestalten, S. 2.

[5] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/05_DER_Detektion_und_Reaktion/DER_2_1_Behandlung_von_Sicherheitsvorfaellen_Edition_2021.pdf?__blob=publicationFile&v=2

[6] Weitere Verpflichtungen – sowohl in Bezug auf die Notwendigkeit eines Vorfallmanagements, weiterer Meldepflichten sowie zur Dokumentation von Vorfällen – können sich unter anderem aus dem BSIG, dem GHB und dem KonTraG ergeben.

[7] Brink, in: Wolff/ Brink, BeckOK Datenschutzrecht, Art. 33, Rn. 62.

[8] Strüve, Datenschutz in der ärztlichen Praxis, 13.5.

Im Rahmen der Rechenschaftspflicht ist es für den Verantwortlichen vorteilhaft alle für diesen Nachweis gegenüber der Aufsichtsbehörde möglicherweise relevanten Daten zu speichern. Darunter befinden sich dann auch vielfältige Daten mit Personenbezug. Primär ist dies beim Dokumentieren der Umstände der Fall, etwa im Rahmen eines Vorfalltickets, welches in der Regel zum Zeitpunkt der internen Meldung eines Vorfalls erstellt wird. Enthalten sind hier die Kontaktdaten betroffener sowie meldender Personen wie Namen, Mail-Adressen und Telefonnummer. Betroffene Personen können hierbei solche sein, die den Vorfall ausgelöst haben oder von diesem in jeglicher Weise betroffen sind. So könnte beispielsweise ein Angriff auf die IT erfolgen, indem der Mailzugang eines Mitarbeiters gehackt wird und dann Mails von diesem Account aus an weitere Mitarbeiter gesendet werden.

Bei einer Dokumentation der Umstände könnten die Kontaktdaten aller Personen, welche eine Mail erhalten haben, sowie die Daten der gehackten Person oder ihres Rechners dokumentiert werden. Weitere personenbezogene Daten können bei der Dokumentation der weiteren Umstände des Vorfalls anfallen. Im Rahmen des unten angeführten Beispielsfalls könnte so die Mail abgespeichert werden, die den Schadcode enthält.

Bei der Beurteilung eines Vorfalls können ebenfalls personenbezogene Daten dokumentiert werden. So wird zwischen den zuständigen Mitarbeitern ein Mailverkehr über den Vorfall entstehen, in denen sie die Umstände des Vorfalls diskutieren. Es kann auch zu Gesprächen kommen, die protokolliert werden. Nach Abschluss des Managements eines konkreten Vorfalls liegt somit eine umfassende Dokumentation der Vorfallbearbeitung vor, die in der Regel eine ganze Reihe personenbezogene Daten enthält.

## 3. Was ist hinsichtlich der Aufbewahrung und Löschung personenbezogener Daten zu beachten?

Aus Sicht des Datenschutzrechts trifft den Verantwortlichen die Pflicht personenbezogene Daten zu löschen oder zu anonymisieren, wenn diese für die vor der Datenerhebung definierten Verarbeitungszwecke nicht mehr erforderlich sind (Art. 5 Abs. 1 lit. e DSGVO). Dies betrifft auch diejenigen personenbezogenen Daten, die im Rahmen der Dokumentation des Vorfallmanagements verarbeitet werden.

Entgegen dieser Pflicht zur Löschung personenbezogener Daten können unter anderem Gesetze, Kollektivvereinbarungen oder Individualverträge die Pflicht zur Aufbewahrung für einen bestimmten Zeitraum vorschreiben. Beispiele hierfür sind § 147 AO, §§ 238, 257 HGB.[9]


Dementsprechend hat der Verantwortliche Regeln festzulegen, die die Speicherdauer personenbezogener Daten auf das erforderliche Mindestmaß beschränken und trotzdem die einschlägigen gesetzlichen Aufbewahrungspflichten umsetzen. Hierbei ist zu beachten, dass – sofern für ein personenbezogenes Datum mehrere gesetzliche Aufbewahrungsfristen einschlägig sind – dieses Datum bis zum Ablauf der längsten einschlägigen Aufbewahrungsfrist zu speichern ist.[10]

Die Bildung von Löschregeln kann auf Basis der in der DIN 66398 beschriebenen Vorgehensweise erfolgen. Der Zweck der Vorgehensweise ist es, den rechtskonformen Löschzeitpunkt personenbezogener Daten (technikneutral) festzulegen.[11] Für die Entwicklung von Löschregeln wird der Datenbestand eines Verantwortlichen zunächst in Datenarten unterteilt. Für jede Datenart wird darauf folgend eine Löschregel definiert. Diese berücksichtigt

[9] Grothe, in Säcker/ Rixecker/ Oetker/Limperg, Münchener Kommentar zum BGB, § 195 Rn. 4; Macit/Selzer, BvD-News 1/20, 53, 54.

[10] Enzmann/Selzer/Spychalski, EDPL 2018, 416, 417.

[11] Hammer, in Jandt/Steidle, Datenschutz im Internet, S. 420.

- den erforderlichen Verarbeitungszeitraum zur datenschutzrechtlichen Zweckerreichung,
- die gegebenenfalls bestehenden Aufbewahrungspflichten und
- die datenschutzrechtlich vertretbare Frist zur Umsetzung der Löschung nach Ablauf der beiden vorgenannten Zeiträume.[12]

## 4. Was ist bei der Festlegung von Löschregeln für die Vorfalldokumentation zu beachten?

Auch für personenbezogene Daten, die im Rahmen der Dokumentation des Vorfallmanagements verarbeitet werden, müssen Verantwortliche Löschregeln festlegen. Hierbei ist zu betonen, dass für die Bildung von Löschregeln alle für einen bestimmten Verantwortlichen in diesem Zusammenhang relevanten Umstände berücksichtigt werden müssen. Nötig ist also eine *Einzelfallbetrachtung*. Dementsprechend erfolgt die nachfolgende Diskussion *exemplarisch*.

### 4.1 Festlegung des erforderlichen Zeitraums zur Zweckerreichung

Bei der Entwicklung von Löschregeln für das Vorfallmanagement liegt die wohl größte Herausforderung in der Festlegung des erforderlichen Verarbeitungszeitraums zur datenschutzrechtlichen Zweckerreichung. Die datenschutzrechtlichen Zwecke der Verarbeitung personenbezogener Daten im Rahmen des Vorfallmanagements bestehen regelmäßig darin den Vorfall zu bearbeiten, bestehende Melde- und Benachrichtigungspflichten zu erfüllen, Schutzmaßnahmen zur Verhinderung von Folgeschäden zu implementieren und den Rechenschaftspflichten und der Beweissicherung nachzukommen.

Verantwortliche stehen hierbei insbesondere vor der Herausforderung zu bewerten, wie lange personenbezogene Daten für die Zweckerfüllung der Rechenschaftspflichten verarbeitet werden dürfen. Im Rahmen des Art. 5 Abs. 2 i.V.m. Art. 24 Abs. 1 DSGVO wird keine zeitliche Grenze festgelegt, bis zu welcher der Verantwortliche die Daten zum Nachweis aufbewahren sollte. Sinnvoll erscheint es, die Haftungsvermeidung als Ausgangspunkt der notwendigen Aufbewahrungsdauer heranzuziehen. Hierbei liegt es im Interesse des Verantwortlichen, mögliche Bußgelder abzuwehren, indem die Konformität seines Handelns durch eine umfangreiche Dokumentation nachgewiesen werden kann. So drohen i.S.d. Art. 83 Abs. 5 lit. a DSGVO Bußgelder bei Verstößen gegen die Grundsätze der Verarbeitung gemäß Art. 5 DSGVO.

Im Rahmen der DSGVO wird jedoch keine konkrete Verjährungsfrist vorgegeben. Das BDSG legt in § 41 Abs. 2 die Anwendbarkeit des OWiG im Fall von Verstößen gegen Art. 83 Abs. 4 bis 6 DSGVO fest. So verjährt eine Verletzung der Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO gemäß Art. 83 Abs. 5 lit. a DSGVO i.V.m. § 31 Abs. 2 Nr. 1 OWiG spätestens nach drei Jahren. Die Frist beginnt i.S.d. § 31 Abs. 3 OWiG mit dem Abschluss der Handlung, die die Ordnungswidrigkeit begründet und damit am Tag der Tat.[13]

Nach Ablauf dieser Frist können Verstöße aufgrund der Verfolgungsverjährung nicht mehr geahndet werden.[14] Ein weiterer in diesem Zusammenhang zu berücksichtigender Faktor ist die Beweislast bei Schadenersatzansprüchen betroffener Personen nach Art. 82 DSGVO, welcher der Verantwortliche im Rahmen der Rechenschaftspflicht unterliegt.

Schadenersatzansprüche aus Art. 82 DSGVO verjähren gem. § 195 BGB regelmäßig innerhalb von drei Jahren.[15] Die regelmäßige Verjährungsfrist beginnt i.S.d. § 199 Abs. 1 BGB mit dem Ende des Jahres, in dem der Anspruch entstanden ist oder von ihm Kenntnis erlangt wurde.

Zusätzlich kann im Rahmen der Beweissicherung unter anderem die Aufbewahrung zur Vermeidung einer Produkthaftung auf Grundlage des ProdHaftG notwendig werden. Hierbei liegt eine verschuldensunabhängige Gefährdungshaftung vor, auf Basis derer Schadenersatz geltend gemacht werden kann. Dieser Anspruch verjährt i. S. d. § 12 Abs. 1 ProdHaftG innerhalb von drei Jahren ab Kenntnis des Ersatzberechtigten, oder ab dem Zeitpunkt, in dem Kenntnis hätte erlangt werden müssen. Auch können sich Aufbewahrungspflichten

[12] Weiterführende Informationen zur Bildung von Löschregeln auf Basis der DIN 66398: Stummer/ Selzer, BvD-News 3/19, 26, 26 u. 29; Macit/Selzer, BvD-News 1/20, 53, 54 f.
[13] Ellbogen, in: Karlsruher Kommentar zum OwiG, § 31, Rn. 23.
[14] Voigt, in: Taeger/ Gabel, DSGVO BDSG, Art. 5 DSGVO, Rn. 44 f.; Schantz, in: BeckOK Datenschutzrecht, Art. 5 DSGVO, Rn 39; Herbst, in: Kühling/ Buchner, DS-GVO BDSG, Art. 5 DSGVO, Rn. 80.
[15] Frenzel, in: Paal/ Pauly, DS-GVO BDSG, Art. 82 DSGVO, Rn. 19; Voigt, in: Taeger/ Gabel, DSGVO BDSG, Art. 5 DSGVO, Rn. 44 f.

aus mit Kooperationspartnern oder – insbesondere im Forschungsumfeld – mit Projektfördergebern geschlossenen Verträgen ergeben.

## 4.2 Aufbewahrungspflichten

Darüber hinaus ist zu prüfen, ob einer Löschung personenbezogener Daten in Vorfalldokumentationen Aufbewahrungspflichten entgegenstehen. In der vorliegenden, exemplarischen Betrachtung gehen die Autorinnen und der Autor davon aus, dass keine solche Aufbewahrungspflichten für die Vorfalldokumentation bestehen.

## 4.3 Datenschutzrechtlich vertretbare Frist zur Umsetzung der Löschung

Schließlich ist die datenschutzrechtlich vertretbare Frist zur Umsetzung der Löschung nach Ablauf der Zweckerreichung und etwaiger bestehender Aufbewahrungspflichten zu ermitteln. Die Speicherung der Vorfalldokumentation erfolgt häufig im Rahmen eines Ticketsystems, in dem eine Löschung oft händisch erfolgen muss. Die Bestimmung der vertretbaren Frist zur Löschung sollte diesen Umstand berücksichtigen.

Darüber hinaus ist das Risiko, das von der Datenspeicherung für die Rechte und Freiheiten der betroffenen Personen ausgeht zu berücksichtigen. Für die Speicherung der Daten im Rahmen des Vorfallmanagements liegt ein geringes bis maximal mittleres Risiko vor. In der Gesamtschau handelt es sich bei der Mehrzahl der personenbezogenen Daten um Stammdaten. Die Speicherung solcher Daten stellt ein eher geringes Risiko dar. Sensible Daten, welche eines höheren Schutzes bedürfen, kommen in der Regel nicht vor, oder höchstens in verhältnismäßig geringem Umfang im Rahmen von Freitextfeldern oder Anhängen. Die Sicherheit der sensiblen Daten wird hierbei meist durch technische und organisatorische Maßnahmen wie restriktive Berechtigungskonzepte und Verschlüsselungen erhöht.[16] Damit kann die Eintrittswahrscheinlichkeit der Risiken für die Rechte und Freiheiten betroffener Personen gesenkt werden, welche sich aus der Speicherung ergeben könnten.

Unter Berücksichtigung der Risikobewertung, sowie der Verhältnismäßigkeit der Maßnahmen zur Löschung zugunsten des Verantwortlichen, sollten die Prozesse zur tatsächlichen Umsetzung der Löschung nicht länger als ein Jahr dauern.

| **Beispielhafte Löschregel für die Vorfalldokumentation[17]** | |
|---|---|
| Inhaltlicher Umfang | Die Löschregel umfasst alle Datenobjekte, die im Rahmen des Vorfallmanagements gespeichert werden, um Vorfälle ab deren Meldung zu bearbeiten. |
| Verwendungszwecke | • Bearbeitung des Vorfalls<br>• eventuell Erfüllung von Melde- und Benachrichtigungspflichten<br>• eventuell Ergreifen von Schutzmaßnahmen zur Verhinderung von Folgeschäden<br>• Rechenschaftspflichten und Beweissicherung<br>- Art. 5 Abs. 2 DSGVO i.V.m. § 195 BGB, § 31 Abs. 2 Nr. 1 OWiG<br>- § 12 ProdHaftG |
| Zeitraum bis zur vollständigen datenschutzrechtlichen Zweckerreichung | Vollständiger Abschluss der Vorfallbearbeitung und Ablauf aller relevanter Verjährungsfristen (meist nach drei Jahren ab dem Ende des Jahres, in dem der Anspruch entstanden ist). |
| Aufbewahrungspflichten | - |
| Frist zur Umsetzung der Löschung | 1 Jahr |

Tabelle 1: Löschregel für die Datenschutz- und Informationssicherheitsvorfalldokumentation

[16] Stummer/Selzer, BvD-News 3/19, 26, 29.

[17] Die Tabelle ist angelehnt an die DIN 66398, jedoch stark vereinfacht und verkürzt.

## 5. Wie kann eine Löschregel für die Vorfalldokumentation aussehen?

Wie bereits betont ist die Bildung von Löschregeln abhängig von branchenspezifischen rechtlichen Vorgaben zur Aufbewahrung und muss unter allen für die Organisation/das Unternehmen relevanten Umstände vorgenommen werden. Insofern stellen die Autorinnen und der Autor dieses Beitrags nachfolgend eine *exemplarische* Löschregel vor, die eine Orientierung für eine Vielzahl von Organisationen sein dürfte, jedoch keine branchen- und organisationsspezifischen Anforderungen abbildet.

Es ist grundsätzlich möglich im begründeten Ausnahmefall von einer zuvor definierten Löschregel abzuweichen, zum Beispiel im Falle eines noch offenen Rechtsstreits (etwa Strafverfolgung eines Angreifers) für den die Vorfalldokumentation als Beweismittel dienen soll. Für diese Fälle muss individuell geklärt werden, ob und wie lange die vordefinierte Löschregel der Vorfalldokumentation überschritten werden muss oder darf. Dieser Schritt sollte wiederum dokumentiert werden.

### Über die Autor*innen


**Louisa Rudolph**
Informationsjuristin (LL.B.), E-Mail:
louisa.rudolph@zv.fraunhofer.de

**Dr. Annika Selzer**
Gruppenleiterin für Informationsrecht und interdisziplinäre Recht-Technik-Forschung am Fraunhofer-Institut für Sichere Informationstechnologie (SIT), E-Mail:
annika.selzer@sit.fraunhofer.de

**Dr. Ulrich Pordesch**
Bereichsleiter für Sicherheit der Fraunhofer Gesellschaft, Informationssicherheits- und Datenschutzkoordinator der Fraunhofer-Gesellschaft, E-Mail:
ulrich.pordesch@zv.fraunhofer.de

www.sit.fraunhofer.de

Fraunhofer SIT

# TIPPS ZUR COOKIE-COMPLIANCE

Robert Sindlinger, Lukas Rottleb, Dr. Christoph Bausewein


Im Mai 2021 verschickte die Nichtregierungsorganisation "NOYB – europäisches Zentrum für digitale Rechte" mit Sitz in Österreich, die sich der Durchsetzung des Datenschutzes innerhalb der Europäischen Union verschrieben hat, Beschwerden an über 500 Webseitenbetreiber wegen vermeintlich nicht rechtskonformer Cookie-Banner.

Den Webseitenbetreibern wird vorgeworfen Nutzern ihrer Webseiten bei der Anwendung und Nutzung von Cookies und anderen gebräuchlichen Tracking-Technologien in Bezug auf die EU-Datenschutz-Grundverordnung (DSGVO) unzureichend Informationen offenzulegen und keine angemessenen Wahlmöglichkeiten einzuräumen. NYOB hat den betroffenen Webseitenbetreibern eine einmonatige Frist zur Schaffung von Abhilfe gewährt und für den Fall des fruchtlosen Ablaufs eine Beschwerde zur jeweils zuständigen Aufsichtsbehörde angedroht.

Nach offiziellen Angaben möchte NYOB mit der Kampagne dem "Cookie Banner Terror" Einhalt gebieten. Was dies bedeutet und wie dem vorgebeugt werden kann, soll dieser Beitrag beleuchten.

## Cookie Consent Tool

Cookies sind ausweislich zahlreicher Cookie Policies und Erklärungen kleine Textdateien, die beim Besuch einer Internetpräsenz auf dem Computer oder mobilen Gerät gespeichert werden, wie es in etwa auf der Webseite der Europäischen Kommission nachzulesen ist.[1] Weiter heißt es dort zu Cookies sinngemäß:

> *Jedes Mal, wenn Sie die Webseiten besuchen, werden Sie aufgefordert, Cookies zu akzeptieren oder abzulehnen.*
>
> *Mithilfe der Cookies kann sich die Webseite Ihre Einstellungen (wie Benutzername, Sprache usw.) für einen bestimmten Zeitraum merken.*
>
> *Dadurch brauchen Sie diese beim Navigieren auf der Webseite während desselben Besuchs nicht erneut vorzunehmen.*
>
> *Cookies können auch zur Erstellung anonymisierter Statistiken über die Browsing-Aktivitäten unserer Webseitenbesucher verwendet werden.*

Cookies sind datenschutzrechtlich relevant, weil mit ihnen eine Verarbeitung von personenbezogenen Daten einhergehen kann. Erschwerend kommt hinzu, dass noch nicht abschließend geklärt ist, ob oder für welche Anwendungsbereiche für den Einsatz von Cookies die Vorgaben der DSGVO oder des Telemediengesetzes (TMG) maßgeblich sind. Rechtsprechung und Datenschutz-Aufsichtsbehörden geben auf diese Fragen keine abschließenden und teilweise widersprüchliche Antworten.[2]

Nach § 15 Abs. 3 Satz 1 TMG darf der Diensteanbieter für Zwecke der Werbung, Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer nach einer Unterrichtung über sein Widerspruchsrecht dem nicht widerspricht.

Dazu hat der Bundesgerichtshof (BGH) in seinem Urteil vom 28.5.2020 in der Rechtssache Planet49 (Az. I ZR 7/16) klargestellt, dass die Einholung der Einwilligung mittels eines voreingestellten An-

[1] https://ec.europa.eu/info/cookies_de.

[2] So Wybitul/Halim/Böhm unter https://de.lw.com/thoughtLeadership/Das-Cookie-Einwilligung-II-Urteil-des-BGH-Planet49.

kreuzkästchens mit wesentlichen Grundgedanken des § 15 Abs. 3 Satz 1 TMG nicht vereinbar ist. Mithin muss seit besagtem Urteil ein Webseitennutzer zur Nutzung von Cookies und anderer Tracking-Technologien eine informierte, ausdrückliche Einwilligung erteilen, bevor solche installiert und aktiviert werden dürfen.

In der Konsequenz müssen Webseitenbetreiber seit der Rechtsgültigkeit des BGH-Urteils zusätzliche Maßnahmen ergreifen, um diesem Umstand Rechnung zu tragen. Das Gros der Webseitenbetreiber setzt zu diesem Zweck sogenannte Cookie Consent Tools ein, die mit Cookie-Banner-Lösungen arbeiten, die wiederum anbieterabhängig neben der Informations- und Einwilligungsfunktion gleichsam teils Lösungen zum Einwilligungsmanagement, Funktionen zum flexiblen Banner-Design, Webseiten-Scanner, Funktionen zum A/B-Testing zwecks Erprobung und Bewertung verschiedener Designs sowie Lösungen für Präferenzmanagement zum Aufruf und Aktualisierung der festgelegten Nutzerpräferenzen für Desktop und mobile Geräte anbieten. Die Anwendung entsprechender Lösungen erfordert nicht selten gewisse Expertise und Sorgfalt. Dementsprechend sind Rundumsorglospakete wie in anderen Bereichen Mangelware. Anwendern ist daher abzuraten unreflektiert vorgefertigte Lösungen einzusetzen, wie der Beitrag von Meffert über "Consent Tools für Webseiten im Praxistest" in der BvD-News 1/2021 herausgearbeitet hatte. Dabei ist Meffert allerdings nicht im Detail darauf eingegangen, welche Ursache die von ihm festgestellten Rechtsverstöße hatten. Diese Lücke beabsichtigt dieser Beitrag zu schließen, indem er weitergehende Tipps zur Cookie-Compliance und Anwendung von Cookie Consent Tools gibt.

## Cookie-Banner

Cookie-Banner können als Cookie-Warnung bezeichnet werden, die auf Webseiten auftauchen, wenn ein Nutzer die Webseite besucht. Idealerweise soll er im Hinblick auf die dargestellte Rechtslage Auskunft darüber geben, welche Cookies und Tracker verwendet werden, und Nutzern ermöglichen ihre Präferenz bei der Anwendung und Nutzung von Cookies und anderen Tracking-Technologien mitzuteilen. Zwar mögen Cookie-Banner bei Webseitnutzern nicht immer Freude auslösen. Deswegen aber von "Cookie Banner Terror" zu sprechend ist polemisch und erscheint bei gewissenhafter, ordnungsgemäßer Gestaltung des Banners in Erfüllung sämtlicher Pflichten als ungerechtfertigt. Auch Mefferts Feststellung, dass Cookie Consent Tools überbewertet seien und das Vertrauen in sie nicht gerechtfertigt ist, kann nicht ohne Weiteres substantiiert werden. Damit es nicht zu einem "Cookie Banner Terror" kommt, ist es wichtig folgende Aspekte zu beachten:

### Einfügen einer „Alle ablehnen" Schaltfläche in das Cookie-Banner

Abhängig von der individuellen Konfiguration der Webseite muss unter Umständen mehr als eine Bannervorlage genutzt und entsprechend aktualisiert werden. Dabei sollte stets eine Schaltfläche „Alle ablehnen" im Banner eingebunden werden.

Die deutsche Datenschutzkonferenz (DSK) vertritt diesbezüglich folgende Auffassung:

- Cookie-Banner, die Informationen über Cookies und eine „Akzeptieren"-Schaltfläche, aber keine Option zur Ablehnung des Setzens von Cookies bieten, werden als nicht ausreichend angesehen.
- Eine „Alle akzeptieren"-Option sollte mit einer Möglichkeit gepaart sein, Cookies granular abzulehnen.
- Schweigen oder Untätigkeit kann nicht als Einwilligung interpretiert werden; die Einwilligung muss aktiv erteilt werden.[3]

Engere Anforderungen werden darüber hinaus von anderen europäischen Aufsichtsbehörden vertreten, die dann Berücksichtigung finden sollten, wenn die Webseite keinen ausschließlich deutschen Fokus hat und wahrscheinlich auch in anderen Ländern genutzt wird. So proklamiert etwa die französische Datenschutzbehörde *Commission Nationale de l'Informatique et des Libertés* (CNIL) folgende zusätzlichen Bedingungen:

- An sich muss es genauso einfach sein die Tracking-Technologien zu akzeptieren wie sie abzulehnen.
- Wenn die implizite Ablehnung von Cookies respektiert wird (etwa durch Schließen des Banners), müssen die Benutzer darüber informiert werden.[4]

[3] https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf.
[4] https://www.cnil.fr/sites/default/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf.

Vom irischen *Data Protection Commissioner* (DPC) stammen ferner folgende Vorgaben:

- Wenn auf dem Banner eine Schaltfläche mit einer „Akzeptieren"-Option vorhanden ist, muss die Webseite eine Option gleichwertig hervorheben, die es dem Benutzer ermöglicht, Cookies "Abzulehnen", oder eine, die es ihm ermöglicht, die Cookies in einem anderen Layer zu verwalten.
- Webseiten müssen zumindest Informationen bereitstellen, die es dem Nutzer ermöglichen, nicht benötigte Cookies abzulehnen oder weitere Informationen über die Verwendung von Cookies anzufordern.[5]

Allen europäischen Aufsichtsbehörden ist indes die Haltung gemeinsam, dass im Zeitpunkt des Aufrufens der Webseite bis zum Zeitpunkt der Einwilligung des Benutzers keine Informationen erhoben oder Cookies gesetzt werden dürfen. Erst wenn der Benutzer einwilligt, kann die Webseite die Cookies auf dem Gerät des Benutzers ablegen.

## Einholung und Management von Einwilligungen

Nicht jede Cookie-Webseiten-Lösung bietet die Möglichkeit die Einwilligungen von Webseitennutzern einzuholen und zu managen. Dies ist aber aus Gründen der Rechenschaft und Beweisführung relevant und kann über Erfolg oder Misserfolg in behördlichen oder gerichtlichen Auseinandersetzungen entscheiden. Des Weiteren stellt ein Opt-In-Einwilligungslösung sicher, dass standardmäßig keine Cookie-Kategorien aktiviert sind.

Anspruchsvolle Cookie Consent Tools bieten durch Geo Targeting die Möglichkeit, Webseitennutzer an unterschiedlichen Standorten angemessen anzusprechen, indem ein Banner mit der Cookie-Einwilligung angezeigt wird, der den rechtlichen Anforderungen des jeweiligen Landes entspricht. So kann das Einwilligungsmodell basierend auf dem Standort des Benutzers flexibel konfiguriert und angezeigt werden.

Die Geolokalisierungsrichtlinie ermöglicht es ferner Regeln zu definieren, die für verschiedene Regionen gelten. Diesbezüglich ist es relevant, dass derartige Regeln vom Anwender individuell, in Übereinstimmung mit den anwendbaren Vorgaben innerhalb der Geolokalisierungsrichtlinie angepasst, überprüft und regelmäßig aktualisiert werden.

Folglich ist Best Practice ein anpassbares, geolokalisierungsbasiertes Cookie-Banner anzuzeigen, das Cookies automatisch blockiert, bis EU-Besucher die Cookies akzeptieren oder ablehnen. Denn seit dem EuGH-Urteil in der Rechtssache *Planet49*[6] vertritt nicht nur die DSK, sondern auch andere europäische Datenschutzaufsichtsbehörden, darunter die französische und irische, dass vorangekreuzte Kästchen keine gültige Einwilligung darstellen.[7]

## Konfiguration von Schaltflächenfarben und -kontrasten

Das Layout, die Gestaltung, der Inhalt und das Verhalten der Bannervorlage müssen ebenfalls individuell angepasst werden. Auf diese Weise können die Verantwortlichen nicht nur sicherstellen, dass das Erscheinungsbild dem Branding, sondern auch den jeweiligen Maßgaben und Verhaltenspräferenzen entspricht. Als Vorgehensweise empfiehlt sich hier sicherzustellen, dass jede „Akzeptieren"-Schaltfläche die gleiche Hervorhebung und Farbgebung erfährt wie eine „Ablehnen"-Schaltfläche. Es ist daher empfehlenswert für beide Schaltflächen die gleichen Farbkombinationen zu verwenden. Die Kontrastanforderungen der Richtlinien für barrierefreie Webinhalte (Englisch: Web Content Accessibility Guidelines – WCAG) ändern sich je nach Textgröße.[8] Was die Konfiguration von Schaltflächenfarben und -kontrasten anbelangt, vertreten die europäische Datenschutzaufsichtsbehörden unterschiedlich weitgehende Ansichten, die abhängig vom Anwendungsbereich Berücksichtigung finden sollten.

Während die DSK lediglich die Auffassung vertritt, dass ein einfaches Banner mit Cookie-Informationen und einem „Akzeptieren"-Button nicht ausreichend[9] ist, verlangt die CNIL:

- Design und die Oberfläche, die zur Erfassung der Entscheidung des Benutzers verwendet werden, dürfen nicht irreführend sein, so dass eine Wahlmöglichkeit gegenüber einer anderen hervorgehoben wird.
- Beide Auswahlmöglichkeiten (Ablehnen/Akzeptieren) müssen in der gleichen Schriftart und

[5] https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%200n%20cookies%20and%20other%20tracking%20technologies.pdf.

[6] EuGH, Urteil des Gerichtshofs (Große Kammer) v. 1.10.2019, C-673/17, Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. gegen Planet49 GmbH.

[7] https://www.cnil.fr/fr/questions-reponses-lignes-directrices-modificatives-et-recommandation-cookies-traceurs; https://www.dataguidance.com/legal-research/cjeu-verbraucherzentrale-bundesverband-ev-v-planet49-gmbh-1-october-2019.

[8] https://www.w3.org/WAI/WCAG21/Understanding/contrast-minimum.html.

[9] https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf.

Farbe dargestellt werden, leicht lesbar sein und identisch hervorgehoben werden; damit soll dem sogenannten Nudging (*zu Deutsch: Anstoßen, Schubsen*) vorgebeugt werden.[10]

Darüber hinaus verlangt die irische DPC:[11]

- Webseiten dürfen keinen Banner verwenden, der einen Benutzer dazu bringt Cookies eher zu akzeptieren als abzulehnen. Wenn eine Schaltfläche auf dem Banner mit einer „Akzeptieren"-Option verwendet wird, muss der Option, die es dem Benutzer ermöglicht, Cookies „abzulehnen", die gleiche Bedeutung beigemessen werden.
- Erwägungen der Barrierefreiheit sind bei der Gestaltung der Cookie-Banner zu berücksichtigen. So ist das Cookie-Banner etwa mit Benutzern zu testen, die Seh- oder Leseschwächen haben, damit das Banner so zugänglich wie möglich für alle Benutzer entwickelt wird.
- Bei binären, farbcodierten Schiebereglern oder Schaltflächen, die eine Ja- Nein-Option oder eine Ein- und Aus-Option verwenden, ist zu beachten, dass diese Farbschemata nicht immer zugänglich oder selbsterklärend für Benutzer sind.

Insofern kann es sinnvoll sein in einem Cookie-Banner eine Option einzubauen, mit der die Benutzer die Einstellungen anpassen können, indem sie entweder auf einen Link oder eine Schaltfläche innerhalb des Banners klicken.

### Aktualisieren von Cookie-Kategorisierungen

Damit eine Einwilligung gültig ist, müssen Cookies korrekt kategorisiert und angezeigt werden. Um das sicherzustellen, ist der Einsatz eines Scanners empfehlenswert und bei der Auswahl eines geeigneten Cookie Consent Tools zu berücksichtigen, um Cookies und Tracking-Technologien auf der entsprechenden Webseite zu identifizieren und zu kategorisieren. Allerdings ist auch dabei stets zu beachten, dass ein solches technisches Hilfsmittel eine Kontrolle und einen Abgleich mit den tatsächlich im Einsatz befindlichen Cookies und Tracking-Technologien durch den Webseitenanbieter nicht entbehrlich macht. Vorsicht ist besser als Nachsicht lautet die empfohlene Maßgabe.

## Fazit

Es gibt weder Cookie-Banner noch technische Probleme, es gibt lediglich Anwenderprobleme. Der Fokus beim Aufbau und Betrieb einer Webseite darf nicht einzig auf Haptik und Optik liegen, sondern sollte auch auf Compliance – insbesondere Datenschutz-Compliance – gerichtet sein. Dementsprechend bedarf es beim Aufbau und Betrieb einer Webseite der angemessenen Einbindung eines darauf spezialisierten und fachlich versierten Datenschutzbeauftragten oder Datenschutzfachkundigen als Mitgestalter und Lotse. Individuelle, maßgeschneiderte Information zur Anwendung und Nutzung von Cookies und der damit einhergehenden Datenverarbeitung gibt es nur für wenige Sachverhalte aus der Konserve und müssen regelmäßig stattdessen individuell entwickelt und geprüfte werden. Ebenso sollte mit dem Datenschutzbeauftragten abgestimmt werden, nach welcher Maßgabe und zu welchem Zeitpunkt Cookies platziert werden dürfen und wie zu diesem Zweck erteilte Einwilligungen sachgerecht verwaltet werden müssen, um im Bedarfsfall abrufbar und vorlegbar zu sein.


Über die Autoren:

**Robert Sindlinger, CIPP/E**
Country Manager Germany & Austria, OneTrust

**Lukas Rottleb, CIPP/E, CIPM**
Solutions Engineering Lead, OneTrust

**Dr. Christoph Bausewein, CIPP/E:**
BvD-Vorstandsmitglied und Director & Counsel, Data Protection & Policy bei CrowdStrike


[10] https://www.cnil.fr/sites/default/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf.
[11] https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%200n%20cookies%20and%20other%20tracking%20technologies.pdf.

# MITTELSTAND-DIGITAL

## Initiative IT-Sicherheit in der Wirtschaft

Christian Munk

Die Initiative IT-Sicherheit in der Wirtschaft als zweite Säule des Förderschwerpunkts Mittelstand-Digital des Bundesministeriums für Wirtschaft und Energie bietet KMU, Handwerk und Freiberuflern umfassende Unterstützung: Informationen, Werkzeuge und Handreichungen zu den vielfältigen Dimensionen der IT-Sicherheit im Mittelstand stehen im Zentrum des Portfolios. Neben den technologischen, organisatorischen und personellen Handlungsfeldern werden auch damit verbundene Aspekte des Datenschutzes aufgegriffen: IT-Sicherheit und Datenschutz sollten bei Digitalisierungsvorhaben so noch leichter von Grund auf gemeinsam mitgedacht werden können. Die kostenfreien Angebote der Initiative und ihrer Förderprojekte können für Datenschutzbeauftragte wertvolle Beiträge leisten, um den unternehmerischen Datenschutzalltag adäquat zu gestalten.

### Digitalisierung und damit verbundene Bedrohungen nehmen zu

Rund ein Drittel der Mittelständler hat seine Digitalisierungsbemühungen in der Corona-Pandemie erhöht, heißt es im KfW-Digitalisierungsbericht Mittelstand 2020. Einen Onlinehandel auf- oder auszubauen, um auch in Zeiten von Lockdown und Kontaktbeschränkungen weiterhin Kunden erreichen zu können sowie Homeoffice und Videokonferenztechnik für Mitarbeiterinnen und Mitarbeiter standen im Fokus zahlreicher Unternehmen. Dabei scheinen insbesondere die Branchen aus der Not eine Tugend gemacht zu haben, die von der Pandemie besonders betroffen waren, das Dienstleistungsgewerbe etwa oder der Handel.

Doch bereits Videokonferenztechnik etablierter Anbieter zu nutzen, kann Mittelständler nicht zuletzt aufgrund jüngerer kritischer Bewertungen durch Landes-Datenschutzbeauftragte vor herausfordernde Fragen stellen: Ist die Technik sicher und datenschutzkonform, sind spezielle Sicherheitsvorkehrungen erforderlich? Arbeiten im Homeoffice erfordert zusätzliche IT-Sicherheitsmaßnahmen. Zusätzliche Endgeräte sowie die Verbindungen von den Homeoffice-Arbeitsplätzen zum Unternehmen müssen gesichert werden. Ein ungenügendes Bild bei der Umsetzung technischer und organisatorischer Maßnahmen stellt aktuell das Bundesamt für Sicherheit in der Informationstechnik aufgrund einer repräsentativen Befragung fest: Zu viele Unternehmen vernachlässigen die IT-Sicherheit im Homeoffice, insbesondere kleinere und kleinste Mittelständler. Mehr als die Hälfte der Unternehmen investiert mit weniger als 10 Prozent der IT-Ausgaben zu wenig in die Cybersicherheit.

Doch auch ohne Pandemie gilt allgemein: Zunehmende Digitalisierung bedeutet naturgemäß auch weitere Tatmöglichkeiten für Cyberkriminelle: Das Bundeskriminalamt hat im vergangenen Jahr 108.000 Fälle von Cyberkriminalität (7,9 Prozent) mehr als noch 2019 verzeichnet, wobei insbesondere in der Wirtschaft von einem sehr großen Dunkelfeld auszugehen ist. Angriffe auf die Wirtschaft sind bislang überwiegend finanziell motiviert. Auch KMU und Handwerk sind vor Bedrohungen durch Cyberkriminalität nicht gefeit, auch wenn zahlreiche Mittelständler die Ansicht vertreten, das eigene Unternehmen sei zu klein oder zu unbekannt, um Ziel von Hackerangriffen zu werden. Auch kleine und kleinste Unternehmen können für Cyberkriminelle lohnenswerte Ziele sein. Eine von der Initiative IT-Sicherheit in der Wirtschaft des BMWi geförderte Studie des Kriminologischen Forschungsinstituts Niedersachsen zeigt: Das Risiko eines Cyberangriffs steigt mit der Anzahl der Unternehmensstandorte im Inland, mit Standorten im Ausland, Exporttätigkeit oder Aspekten, die bei Cyberkriminellen besonderes Interesse wecken, wie einzigartige Produkte, Patente, Reputation oder ein interessanter Kundenkreis. Möglichen Angriffsszenarien sind dabei oft kaum Grenzen gesetzt: Phishing, also der Diebstahl von Daten durch Täuschen von IT-Anwendern, sonstige Schadsoftware oder Ransomware, mit der Unternehmens- oder Kundendaten rechtswidrig verschlüsselt werden, um mitunter hohe Lösegelder zu erpressen, sind die häufigsten Angriffsszenarien

gegen deutsche Mittelständler. Für den Mittelstand können Cyberangriffe rasch existenzbedrohend werden: Ihr Know-how und ihre Geschäftsmodelle können gefährdet, ihre finanzielle Leistungsfähigkeit über Gebühr beansprucht werden. Auch im Schadensfall sind ihre Herausforderungen oft ungleich höher als die der größeren Unternehmen: Ohne eigene IT-(Sicherheits)-Abteilung und eher geringerem Datenschutz-Know-how ist eine rasche Reaktion im Falle von Cyberkriminalität deutlich erschwert.

## Transferstelle IT-Sicherheit im Mittelstand: IT-Sicherheit passgenau erhöhen

Mittelständler stehen häufig vor der zusätzlichen Herausforderung, die große Vielfalt gewerblicher Angebote zur IT- und Datensicherheit nicht ausreichend bewerten zu können. Beworben werden zahlreiche Produkte auch mit verkaufsfördernden Labels, die mitunter auf Erfordernisse durch die DSGVO verweisen. Welche Lösungen für das eigene Unternehmen relevant sind, um ein adäquates Sicherheitsniveau zu erreichen, welche Angebote hohe Kosten verursachen und nicht bedarfsorientiert sind, können Mittelständler deshalb häufig nur mithilfe externer Experten beurteilen, die sie mitunter nur zurückhaltend hinzuziehen. Die vom BMWi geförderte Transferstelle IT-Sicherheit im Mittelstand soll den Angebotsdschungel für KMU, Handwerk und Freiberufler lichten: Sie bereitet bestehende Angebote Dritter adressatengerecht auf und vermittelt sie anbieterneutral und passgenau auf die spezifischen Bedarfe des Rat suchenden Mittelständlers.

Ganz überwiegend verweist sie auf kostenfreie Angebote, um insbesondere den Unternehmen, die sich bisher noch nicht vertieft mit der IT-Sicherheit befasst haben, niedrigschwellig begegnen zu können. Die Transferstelle möchte den Mittelstand damit in die Lage versetzen, personelle, technische und organisatorische Elemente der IT-Sicherheit und damit zusammenhängender Datenschutzaspekte eigenständig adäquat fortzuentwickeln. Die Transferstelle IT-Sicherheit im Mittelstand wird von Deutschland sicher im Netz, dem DIHK, der Hochschule Mannheim sowie Fraunhofer FOKUS und IAO betrieben. Ihre Angebote sind kostenfrei auf ihrer Website erhältlich. Die Transferstelle ist Bestandteil der Mittelstandsstrategie des BMWi.

Das Herzstück der Transferstelle ist der nicht nur sprachlich an den Wahl-O-Mat angelehnte Sec-O-Mat: Das Online-Werkzeug erfragt Eckdaten des Unternehmens, unterbreitet auf Grundlage Künstlicher Intelligenz Umsetzungsvorschläge und verweist auf konkrete – ganz überwiegend kostenfreie – Maßnahmen. Auch verschiedenste Produkte zu Datenschutz und Informationssicherheit sind im Angebot: Checklisten und Informationsmaterialien etwa oder Werkzeuge, um sich als Mittelständler im großen Feld des Datenschutzes zurechtzufinden. Die enthaltenen regionale Angebote können dazu beitragen Hemmschwellen im Mittelstand zu senken. Zudem steht der Angebotskatalog offen: Weitere Angebote können vorgeschlagen und von der Transferstelle kuratiert werden. Auch die bedeutende Sensibilisierung von Mitarbeiterinnen und Mitarbeitern zu Datenschutz, Datensparsamkeit oder möglichen Einfallstoren für Cyberkriminelle wird adressiert. Die Arbeit mit dem Sec-O-Mat ist längerfristig angelegt: Routen zeigen individuelle Wegstrecken auf, auf denen sich Mittelständler fortentwickeln können.

Am Anfang einer solchen mittel- oder langfristigen Entwicklung steht häufig eine Bestandsaufnahme: Mit dem vom BMWi geförderten Online-Werkzeug CARE des Kriminologischen Forschungsinstituts Niedersachsen können Mittelständler auf Grundlage empirischer Studiendaten ihr individuelles Risikoprofil mit wahrscheinlichen Angriffsszenarien erstellen. Das Werkzeug und die zugrundeliegende Studie sind über die Website der Initiative IT-Sicherheit in der Wirtschaft verfügbar.

IT-Sicherheit und Datenschutz sind sensible Themen, die viele Menschen vorzugsweise persönlich und nicht am Telefon oder über Online-Kanäle besprechen möchten. Deshalb hat die Transferstelle regionale Anlaufstellen eingerichtet: Rund 40 dieser Regionalstandorte sind deutschlandweit für Mittelständler da. Unmittelbar nach Erscheinen dieser Ausgabe bringt die Transferstelle die Themen IT- und Cybersicherheit auch auf die Straße: KMU, Handwerk und Freiberufler erreicht das Mobil auch fernab der Standorte in den Regionen zum persönlichen Gespräch.

## Förderprojekte für Mittelständler

Während die Transferstelle Angebote Dritter vermittelt, steht die zweite Säule der Initiative für Innovationen in Sachen Cybersicherheit und damit verbundene Datenschutzaspekte: Sie fördert Einzel- und

Verbundprojekte nicht gewinnorientiert arbeitender Organisationen zur IT-Sicherheit von KMU und Handwerk mit dem Ziel, digitale Prozesse und Geschäftsmodelle sicher einsetzen zu können. Hochschulen, außeruniversitäre Forschungseinrichtungen, Verbände oder Kammern bringen ihr Wissen und ihre Erfahrungen aus Forschung und Praxis in innovative und anwendungsorientierte Werkzeuge und Materialien ein. Neben konkreten innovativen Angeboten für Mittelständler unterstützt die Initiative IT-Sicherheit in der Wirtschaft so auch anwendungsorientierte wissenschaftliche Forschung zur IT-Sicherheit.

Zehn aktive und geplante Projekte erarbeiten derzeit Lösungen zur Sensibilisierung und Qualifizierung sowie technische Werkzeuge. Lernszenarien für mögliche Bedrohungen, IT-Sicherheitsspiele oder eine Weiterbildungsplattform für IT-Sicherheit sollen Mittelständler unterstützen den Faktor Mensch in den Mittelpunkt ihrer IT-Sicherheitsstrategie zu stellen. Andere Projekte erleichtern den Zugang zum IT-Grundschutz oder erarbeiten spezifische Lösungen für bestimmte Wirtschaftszweige. Ein neu geplantes Projekt soll durch Normung die Beratungsqualität von IT-Dienstleistern zur IT-Sicherheit erhöhen. Alle Projektinformationen und -ergebnisse sind über die Websiten der Initiative IT-Sicherheit und der Transferstelle kostenfrei erhältlich.

## Resümee

Die Initiative IT-Sicherheit in der Wirtschaft adressiert als zweite Säule des Förderschwerpunkts Mittelstand-Digital die Handlungsfelder Sensibilisieren, Qualifizieren und Umsetzen von IT-Sicherheit und damit verbundener Datenschutzaspekte. Mit der Transferstelle IT-Sicherheit im Mittelstand und verschiedenen Einzel- und Verbundprojekten erhalten KMU, Handwerk und Freiberufler praxisorientierte und kostenfreie Unterstützungsangebote, um den wachsenden Bedrohungen durch Cyberkriminalität präventiv begegnen zu können. Doch häufig sehen sich Mittelständler durch Kosten für IT-Sicherheit und Datenschutz vor neue Herausforderungen gestellt. Deshalb stellen wir in der nächsten Ausgabe der BvD-News mit dem Investitionszuschussprogramm „Digital Jetzt“ die dritte Säule von Mittelstand-Digital vor.

## Über den Autor

**Christian Munk**
ist Referent im Referat Mittelstand-Digital
des Bundesministeriums für Wirtschaft und Energie

▶ www.it-sicherheit-in-der-wirtschaft.de

IT-Sicherheit IN DER WIRTSCHAFT

**Transferstelle IT-Sicherheit im Mittelstand:**

▶ www.tisim.de

**Sec-O-Mat der Transferstelle:**

▶ https://sec-o-mat.de

Transferstelle IT-Sicherheit im Mittelstand
Einfach. Sicher. Machen.

Empfohlen von

DATENSCHUTZ EXPERTE.DE

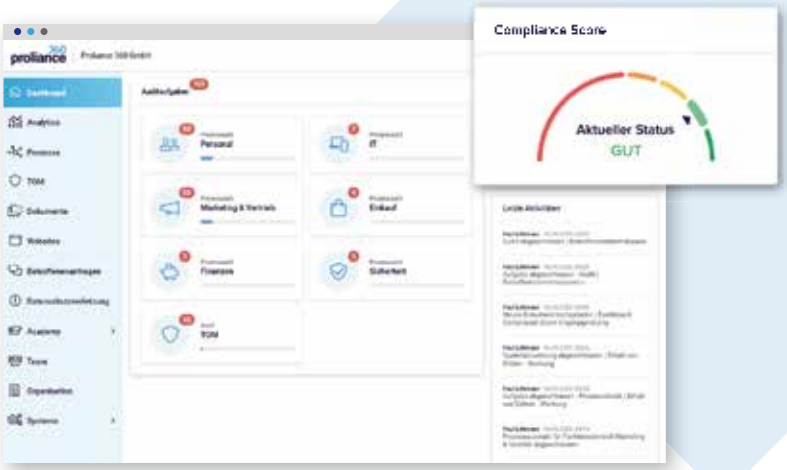
**Ein Freimonat**
**für BvD-Mitglieder**

# Automatisiertes Datenschutzmanagement mit Proliance 360

Datenschutz vorgedacht: Verabschieden Sie sich von Excel und Papier sowie manuellen Arbeitsschritten. Mit Proliance 360 haben Sie die DSGVO im Griff und Ihre Datenschutz-Compliance stets im Blick. Entwickelt mit der Erfahrung aus über 1.500 Kundenprojekten. Nie war es einfacher, Datenschutz zu managen.

## Unser Angebot für Sie

- Das DSGVO-Komplettset: VVT, TOM, Schulungen & Co.
- Datenschutz auf Knopfdruck mit über 25.000 vorgedachten Workflows
- Aufwände durch Smart Legal Tech signifikant reduzieren
- Einfache Bedienung und Einbindung von Teammitgliedern




Weitere Informationen zu Proliance 360 finden sie auf **www.proliance.ai**
Vereinbaren Sie noch heute einen Beratungstermin unter **+49 (0)89 2500 392 20** oder buchen Sie Ihren Slot online mit Hilfe des **QR-Codes.**

PROLIANCE GmbH München, 2021

proliance

# DATENSCHUTZ IN LIECHTENSTEIN

## Umsetzung und Anwendung der DSGVO in einem Kleinstaat

Prof. Dr. Marie-Louise Gächter

Die Datenschutz-Grundverordnung (DSGVO) erlangte am 25. Mai 2018 Geltung in der EU und wurde mit dem EWR-Übernahmebeschluss am 20. Juli 2018 auch in den drei EWR/EFTA-Staaten Island, Liechtenstein und Norwegen wirksam. Damit gilt die DSGVO in den EWR/EFTA-Staaten in gleichem Ausmaß wie in den EU-Staaten. Lediglich in Bezug auf die Teilnahme der drei Staaten im Europäischen Datenschutzausschuss (EDSA) ist festzuhalten, dass die EWR/EFTA-Staaten keine Befugnis haben, den Vorsitz zu übernehmen und auch kein Stimmrecht haben, sondern ihr Votum lediglich zur Kenntnis genommen und dokumentiert wird. Die Praxis der letzten drei Jahre hat allerdings gezeigt, dass diese Einschränkung des Stimmrechts wenig konkrete Auswirkungen hat, denn es steht allen Staaten einschließlich der EWR/EFTA-Staaten frei sich an den Diskussionen zu beteiligen und ihre Meinung zu äußern.

### Besonderheiten des liechtensteinischen Datenschutzgesetzes

Am 1. Januar 2019 trat das liechtensteinische Datenschutzgesetz (DSG) in Kraft, für welches das deutsche Bundesdatenschutzgesetz (BDSG) als Rezeptionsgrundlage gewählt wurde. Die Entscheidung, sich an der deutschen Umsetzung der DSGVO zu orientieren, war ein großer Schritt für Liechtenstein, denn bis zu diesem Zeitpunkt war das Schweizer Datenschutzrecht Vorbild für das bis 2018 geltende nationale Datenschutzgesetz. Lediglich einzelne Artikel des BDSG wurden vom Liechtensteinischen Gesetzgeber anlässlich der Revision 2019 nicht übernommen, so unter anderem die Regelung des Art. 20 BDSG betreffend den gerichtlichen Rechtsschutz. Und in Bezug auf die Verhängung von Bußgeldern hat sich Liechtenstein ausnahmsweise am österreichischen Gesetzgeber orientiert und trotz fehlender Öffnungsklausel in diesem Bereich eine eigene Lösung angestrebt. Während es in Art. 58 Abs. 2 Bst. i DSGVO heißt, dass Bußgelder „zusätzlich zu oder anstelle von in diesem Absatz genannten Maßnahmen, je nach den Umständen des Einzelfalls" zu verhängen sind, bestimmt Art. 40 Abs. 6 DSG, dass „insbesondere bei erstmaligen Verstößen die Datenschutzstelle im Einklang mit Art. 58 der Verordnung (EU) 2016/679 von ihren Abhilfebefugnissen insbesondere durch Verwarnen Gebrauch macht". Diese beiden Besonderheiten waren zwischenzeitlich Gegenstand von Gerichtsentscheidungen.

### EFTA-Gerichtshof, Rs. E-11/19 und E-12/19 – klares Votum Pro Datenschutz

Eine sehr weitreichende und bedeutende Entscheidung betreffend die Parteien in einem Verfahren nach Art. 77 bzw. 78 Abs. 1 DSGVO wurde am 10. Dezember 2020 vom EFTA-Gerichtshof getroffen. Der EFTA-Gerichtshof mit Sitz in Luxemburg entspricht dem Gerichtshof der EU für Angelegenheiten, welche die EWR/EFTA-Staaten betreffen. Er setzt sich aus je einem Richter aus jedem EWR/EFTA-Mitgliedstaat zusammen. Jedes Gericht eines EFTA-Staats, der Vertragspartei des EWR-Abkommens ist, kann dem EFTA-Gerichtshof eine Frage über die Auslegung einer EWR-Rechtsnorm aus dem EWR-Abkommen oder aus Sekundärrecht stellen, wenn es eine darüber zum Erlass seines Urteils für erforderlich hält. Die liechtensteinische Beschwerdekommission für Verwaltungsangelegenheiten (VBK) hatte in einem Beschwerdeverfahren gegen eine Entscheidung der Datenschutzaufsichtsbehörde Liechtenstein (Datenschutzstelle) zu entscheiden. Dabei stellten sich zwei grundlegende Fragen:

- Darf ein Beschwerdeführer im Beschwerdeverfahren gegenüber dem Beschwerdegegner „anonym" bleiben?
- Ist es vereinbar mit den Grundsätzen der DSGVO, dass eine betroffene Person, die Beschwerdeführer im Verfahren nach Art. 77 DSGVO vor der Datenschutzaufsichtsbehörde ist, im darauf folgenden Rechtsmittelverfahren ebenfalls als Partei gilt und bei Unterliegen zum Kostenersatz verpflichtet ist, obwohl das Rechtsmittel vom ursprünglichen Beschwerdegegner (Verantwortlicher im Sinne des Art. 4 Ziff. 7 DSG-VO) ergriffen wurde?

Die Entscheidung des EFTA-Gerichtshofs war eindeutig und kann als Votum für eine Stärkung des Schutzes der betroffenen Personen und der Durchsetzung der Betroffenen-

rechte gewertet werden. Der EFTA-Gerichtshof bejahte die Möglichkeit der Nichtoffenlegung der personenbezogenen Daten des Beschwerdeführers, unter der Voraussetzung, dass dadurch nicht die *«Garantien eines ordnungsgemäßen Verfahrens»* verletzt würden. Gemäß EFTA-Gerichtshof hat ein *«Wirksamer gerichtlicher Rechtsschutz einschließlich des Rechts auf ein faires Verfahren, das einen allgemeinen Grundsatz des EWR-Rechts darstellt, das gleiche Schutzniveau wie Artikel 6 Absatz 1 der EMRK zu bieten»*. Art. 6 der Europäischen Menschenrechtskonvention (EMRK) findet nicht nur in Straf- und Zivilverfahren Anwendung, sondern auch im Verwaltungsverfahren. Das zuständige Gericht oder Behörde muss den Parteien die Möglichkeit gewähren unter wesentlich gleichartigen Bedingungen ihre Prozessstandpunkte effektiv vertreten zu können. Von diesem Recht auf ein faires Verfahren umfasst sind unter anderem der Grundsatz der Waffengleichheit, das Recht auf Akteneinsicht, der Anspruch auf rechtliches Gehör sowie das Recht auf Begründung von Entscheidungen.

Nach der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) ist das Gericht oder die Behörde verpflichtet jede ihnen eingereichte Stellungnahme den Beteiligten zur Kenntnis zu bringen und Gelegenheit zu geben dazu Stellung zu nehmen. Vereinfacht ausgedrückt bedeutet dies, dass ein Verfahren gemäß Art. 77 DSGVO ohne die Offenlegung der Identität des Beschwerdeführers dann durchgeführt werden kann, wenn die Datenschutzaufsichtsbehörde nach sorgfältiger Prüfung festgestellt hat, dass durch die «Anonymität» der Beschwerde der Verantwortliche bzw. Beschwerdegegner keine Einschränkungen in Bezug auf ein faires Verfahren erleidet.

Zur Kostenfrage im Rechtsmittelverfahren stellte der EFTA-Gerichtshof unmissverständlich fest, dass eine mögliche, im nationalen Verfahrensrecht festgesetzte Kostenersatzpflicht dem Recht auf eine unentgeltliche Beschwerde nach Art. 77 Abs. 1 und Art. 57 Abs. 3 der DSGVO entgegensteht und zudem dem Zweck der DSGVO widerspricht einen klar durchsetzbaren Rechtsrahmen zu schaffen und betroffenen Personen in rechtlicher und praktischer Hinsicht mehr Sicherheit zu bieten.

Neben diesen beiden klaren Voten hat das Urteil des EFTA-Gerichtshof aber noch weiterreichende Bedeutung. So etwa stellt der Gerichtshof fest, dass eine Aufsichtsbehörde im Rahmen eines Verfahrens zur Prüfung einer Beschwerde nach Art. 77 DSGVO nicht an das Parteienvorbringen gebunden ist, sondern darüber hinaus auch amtswegige Feststellungen treffen kann, sprich Datenschutzverletzungen aufgreifen kann, die der Beschwerdeführer in seiner Beschwerde gar nicht vorgebracht hat. Diese Möglichkeit ist in der DSGVO nicht explizit vorgesehen und wirft daher immer wieder Fragen auf. Wenngleich in zahlreichen Kommentaren ein solches Vorgehen befürwortet wird, ist die Klarstellung durch den EFTA-Gerichtshof ein deutliches Votum für die Kompetenzen und Entscheidungsbefugnisse der Aufsichtsbehörden.

Für Liechtenstein ist das Urteil des EFTA-Gerichtshofs auch insofern von Bedeutung, als dieses eine eindeutige Stellung bezieht zum Beschwerderecht bzw. Beschwerdeverfahren und der Rolle der Parteien. Es handelt sich um ein Verfahren, in dem die Parteien das Recht auf einen wirksamen gerichtlichen Rechtsschutz einschließlich des Rechts auf ein faires Verfahren haben. Dies mag selbstverständlich sein für die meisten EU-Staaten, es steht aber im Gegensatz zur Rechtslage in der Schweiz, wo das neue totalrevidierte Bundesgesetz über den Datenschutz vom 25. September 2020 (CH-DSG) den betroffenen Personen ein solches Beschwerderecht einschließlich der Parteirechte nicht zuerkennen wird, sondern die Möglichkeit der betroffenen Personen, sich an die Aufsichtsbehörde zu wenden, als bloßes «Anzeigerecht» ausgestaltet ist. Sprich, gemäß Art. 49 CH-DSG eröffnet der EDÖB von Amtes wegen oder auf Anzeige hin eine Untersuchung gegen ein Bundesorgan oder eine private Person, wenn genügend Anzeichen bestehen, dass eine Datenverarbeitung gegen die Datenschutzvorschriften verstoßen könnte. Er kann von der Eröffnung einer Untersuchung absehen, wenn die Verletzung der Datenschutzvorschriften von geringfügiger Bedeutung ist.

## Geldbußen versus Verwarnung

Die Regelung in Art. 40 Abs. 6 DSG, wonach die Datenschutzbehörde insbesondere bei erstmaligen Verstößen im Einklang mit Art. 58 DSGVO von ihren Abhilfebefugnissen insbesondere durch Verwarnen Gebrauch machen wird, war ein Wunsch des liechtensteinischen Gesetzgebers und von der Sorge getragen, dass der Bußgeld-Katalog des Art. 83 DSGVO in einem Kleinstaat wie Liechtenstein nicht größenverträglich sei. Dieses Argument stieß auf wenig Widerstand und schien auch schlagend genug die Regelung in das neue DSG aufzunehmen, obwohl eine Öffnungsklausel dafür in der DSGVO fehlte. Und schließlich hatte man sich ja am Nachbarstaat Österreich orientiert, und zudem besagte der Gesetzeswortlaut nicht, dass in keinem Fall eine Geldbuße vor oder gleichzeitig mit einer Verwarnung auszusprechen wäre. Der zweifach gewählte Begriff «insbesondere» erweckte nicht den Anspruch auf Ausschließlichkeit. Während es in Liechtenstein somit die ersten Jahre ruhig blieb um diese Vorrangregel, musste man auf Kritik in Österreich nicht lange warten und bereits während des

Gesetzgebungsprozesses wurde ihre Vereinbarkeit mit dem Europarecht in Frage gestellt. Schließlich hat auch das österreichische Bundesverwaltungsgericht (BVwG) am 2. März 2020 in einer – noch nicht rechtskräftigen – Entscheidung (E-CLI:AT:BVWG:2020:W211.2217212.1.00) festgestellt, dass § 11 DSG nicht in dem Sinne anzuwenden ist, dass die Datenschutzaufsichtsbehörde bei erstmaligen Verstößen in ihrem Ermessen beschränkt wird. Das Gericht stellte fest, dass sich ein «Vorrang des Vorgehens nach § 11 DSG der Systematik und dem Anwendungsvorrang der DSGVO jedenfalls nicht entnehmen lässt».

Anders ist die Rechtslage nach wie vor in Liechtenstein. Hier hat die VBK im September 2020 Art. 40 Abs. 6 DSG bestätigt und mit ihrer Entscheidung festgestellt, dass der Aufsichtsbehörde wenig Spielraum bleibt. Bei einem erstmaligen Verstoß hat eine Verwarnung im Sinne des Art. 58 Abs. 2 Bst. b DSGVO zu erfolgen und erst im Anschluss an die formelle Verwarnung kann bei einem wiederholten Fehlverhalten eine Geldbuße verhängt werden. Auf die Frage der Verhältnismäßigkeit ging die VBK nicht ein, sondern stellte im konkreten Fall nur das Fehlen einer vorangegangenen expliziten, in schriftlicher Form ausgesprochenen und für den Verantwortlichen als solche erkennbare Verwarnung fest. Die Entscheidung ist rechtskräftig und es bleibt abzuwarten, ob sie auch in künftigen Fällen, in denen es um schwerwiegendere Verletzungen als im konkreten Fall gehen würde, aufrechterhalten werden kann.

## Fazit

Liechtenstein ist der kleinste EWR-Staat, in dem die DSGVO gilt, und die Frage einer Größenverträglichkeit der DSGVO prägte vor allem die Anfangsdiskussionen in der Umsetzung der neuen Bestimmungen, und sie ist nach wie vor nicht ganz verstummt. Gewiss sind die Anforderungen der DSGVO für kleine Institutionen nicht zu unterschätzen, diese finden sich jedoch in jedem Staat, hier ist Liechtenstein nicht die Ausnahme. Und auch bei den zahlreichen Fragestellungen, wie das nationale Verwaltungsrecht mit den Datenschutzbestimmungen in Einklang gebracht werden kann, ist Liechtenstein keine Ausnahme, denn diese Diskussionen prägen die Umsetzung in ganz Europa. Umso grösser ist das Gewicht, das den europäischen Gerichten bei dieser Auslegung zukommt und gerade das EFTA-Gerichtshof-Urteil kann hier als wegweisend betrachtet werden, denn die Luxemburger Richter haben sich klar für den Datenschutz und die Rechte der betroffenen Personen ausgesprochen und in vielfacher Hinsicht klargestellt, welch tragende Rolle die Verfahren haben, wenn es darum geht, dem Datenschutz die Rolle einzuräumen, die ihm als Grundrecht in Europa zukommt.

## Über die Autorin

**Prof. Dr. Marie-Louise Gächter**
ist seit 2018 Leiterin der Datenschutzaufsichtsbehörde des Fürstentums Liechtenstein und Titularprofessorin an der Rechtswissenschaftlichen Fakultät der Universität Fribourg in der Schweiz.



# VIDEOÜBERWACHUNG UNTER GELTUNG DER DS-GVO

Barbara Thiel

*Videoüberwachung ist in unserem Leben bereits allgegenwärtig. Dennoch ist der Drang nach noch mehr Kameras ungebrochen. Auf welche gesetzlichen Regeln können sich Verantwortliche bei der Einführung einer Videoüberwachung stützen? Die Datenschutz-Grundverordnung trägt leider nicht dazu bei eine einfache Antwort auf diese Frage zu finden.*

Im öffentlichen Bereich wird Videotechnik bereits seit vielen Jahren zur Überwachung von Straßen und Plätzen eingesetzt. Hierbei geht es um Orte, die sicherheitskritisch sind oder die eine hohe Kriminalitätsbelastung aufweisen. Auch wenn wir mit dem Auto fahren, werden wir von schier unzähligen Kameras an Ausfallstraßen oder auf Autobahnen überwacht, die dazu dienen sollen Gefahrenlagen frühzeitig zu erkennen und den Verkehrsfluss zu gewährleisten.

Staatliche Videoüberwachung findet außerdem zur Objekt-, Eigen- und Beweissicherung statt. So werden Kitas, Schulen, Universitäten oder Gerichte und Polizeistationen kameraüberwacht. Bedeutung gewinnt die Videoüberwachung auch im Arbeitsalltag der Polizei. Hier sei an die Diskussion zur Einführung der sogenannten Bodycams erinnert. Diese am Körper getragenen Kamera kann die Polizeibeamtin oder der Polizeibeamte einschalten und Bildaufnahmen fertigen, wenn sie oder er in eine gefahrenträchtige Situation kommt. Allein die Anwesenheit der Kamera soll dabei deeskalierend wirken, so jedenfalls die Ansicht der Polizei.

Auch private Stellen setzen vermehrt Videotechnik ein, um insbesondere ihr Eigentum zu schützen oder Straftaten zu verfolgen – etwa in Kaufhäusern, Einkaufspassagen oder auf privaten Grundstücken. Und auch wenn wir mit Bus und Bahn fahren, werden wir von Kameras beobachtet.

## Verbreitung von Videoüberwachung

Zur Zahl von Videoüberwachungsanlagen in Deutschland liegen keine verlässlichen Angaben vor. Eine bundesweite Erhebung wurde bisher nicht durchgeführt und Melde- oder Genehmigungspflichten gibt es dafür nicht. So kann man sich einer Zahl lediglich annähern. Eine gute Quelle hierfür sind Antworten auf verschiedene parlamentarische Anfragen: So waren im Jahr 2013 insgesamt 495 Bahnhöfe der Deutschen Bahn mit rund 3.800 Videokameras ausgestattet.[1] Im Oktober 2016 hatte die Bundespolizei Zugriff auf rund 6.400 Videokameras der DB AG.[2] Allein in Berlin überwachten mit Stand Januar 2016 insgesamt 14.765 Kameras den öffentlich zugänglichen Raum, davon 13.643 den öffentlichen Personennahverkehr.[3] Und eine kleine Anfrage aus dem Februar 2020 ergab, dass allein an allgemeinbildenden und beruflichen Schulen in Hamburg 360 Kameras im Einsatz sind.[4] Es ist zu vermuten, dass die Zahl der Kameras zwischenzeitlich nicht zurückgegangen ist. Dies führt dazu, dass wir bei vielen Gelegenheiten erfasst werden, wenn wir uns im Alltag in der Öffentlichkeit bewegen. Hätte jemand Zugriff auf das gesamte Bildmaterial, ließe sich vermutlich ein detailliertes Bewegungsprofil von nahezu jeder Person in Deutschland erstellen.

## Rechtsgrundlagen

Welche gesetzlichen Regeln gelten nun für die Videoüberwachung? Und was hat sich durch die Datenschutz-Grundverordnung (DS-GVO) geändert? Die europäischen Vorschriften haben hier jedenfalls nur sehr eingeschränkt zu einer Harmonisierung beigetragen. Auch unter Geltung der DS-GVO gibt es bei der Frage, welche Rechtsnorm für den Betrieb einer Videoüberwachungsanlage einschlägig ist, weiterhin eine differenzierte Antwort.

[1] BT-Drs. 17/12318
[2] BT-Drs. 18/10137
[3] Drs. 17/17723
[4] Drs. 21/20102

Entscheidend sind zwei Fragen. Erstens: Wer will die Videoüberwachung einsetzen? Eine nicht-öffentliche Stelle (typischerweise die Wirtschaft oder Privatpersonen) oder eine öffentliche Stelle (typischerweise die Polizei oder sonstige Behörden)? Die zweite Frage lautet: Welchem Zweck dient die Überwachung? Beispiele für bestimmte Zwecke sind: der Schutz des Eigentums oder von Personen, eine Eingangskontrolle oder die Verhütung oder Verfolgung von Straftaten.

Die zentrale Regelung für die Verarbeitung von Daten mittels Videotechnik ist Art. 6 Abs. 1 Buchst. f DSGVO. Sie ersetzt den § 6 b BDSG a. F. als Grundnorm, obwohl das Wort „Videoüberwachung" in Art. 6 DSGVO nicht zu finden ist. Im Kern sind die Regelungen jedoch identisch, denn Daten dürfen im Rahmen einer Videoüberwachung nur verarbeitet werden, wenn

1. der Verantwortliche ein **berechtigtes Interesse** nachweisen kann,

2. die Verarbeitung der Daten zur Wahrung des berechtigten Interesses des Verantwortlichen oder eines Dritten **erforderlich** ist und

3. die von der Videoüberwachung **betroffenen Personen** keine Rechte geltend machen können, die höher zu bewerten sind als das berechtigte Interesse des Verantwortlichen an der Überwachung.

Im Ergebnis ist daher immer eine **Rechtsgüterabwägung** vorzunehmen.

Zudem sind gewisse Formvorschriften zu beachten, die verschärft wurden. Nach altem Recht war die Videoüberwachung gegenüber den betroffenen Personen „nur" kenntlich zu machen. Reichte früher ein Hinweisschild mit einem Videokamera-Symbol aus (Piktogramm), so verlangt das neue Recht wesentlich mehr Informationen, so. z. B. über den Zweck der Datenverarbeitung, über den Verantwortlichen oder über die Rechte der Betroffenen. Die Datenschutzbehörden haben hierfür frühzeitig ein Muster entwickelt und veröffentlicht.

Es gibt allerdings weitere Vorschriften, die es dem Rechtsanwender nicht ganz einfach machen, die richtige Norm für eine Datenverarbeitung mittels Videotechnik zu finden.

## 1.) § 4 BDSG

Wirft man einen Blick in das Bundesdatenschutzgesetz, nämlich in § 4, könnte man glauben, die einschlägige Rechtsgrundlage für eine Videoüberwachung öffentlich zugänglicher Räume gefunden zu haben. Als Adressaten kommen sowohl nicht-öffentliche als auch öffentliche Stellen in Betracht, wobei das BDSG nur Vorgaben für öffentliche Stellen des Bundes, also Bundesbehörden, machen kann. Für Landesbehörden gilt das jeweilige Landesdatenschutzgesetz.

Vorbild für § 4 BDSG war § 6 b BDSG a. F. Dieser wurde 2001 ins Gesetz eingefügt, um die Datenverarbeitung in Form einer Videoüberwachung spezialgesetzlich zu regeln. Im April 2017 wurde diese Norm durch das sog. Videoüberwachungsverbesserungsgesetz um eine Güterabwägungsklausel ergänzt, die sich wortgleich in § 4 BDSG wiederfindet. Danach wird der Schutz von Leben, Gesundheit und Freiheit in bestimmten Situationen als besonders wichtiges Interesse deklariert. Voraussetzung hierfür ist, dass die Videoüberwachung öffentlich zugängliche großflächige Anlagen wie Sportstätten, Einkaufszentren und Parkplätze betrifft oder Fahrzeuge und öffentlich zugängliche großflächige Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs.

Mithilfe einer Klausel zur Abwägungsfiktion wollte der Gesetzgeber dem Schutz der Bevölkerung ein größeres Gewicht beimessen. Hintergrund für das Gesetz waren der Terroranschlag in Ansbach sowie der Amoklauf im Olympiaeinkaufszentrum in München im Juli 2016. Die Politik war der Ansicht, durch eine Ausweitung der Videoüberwachung derartige Gewalttaten besser verhindern oder aufdecken zu können.

Von Anfang an lehnten die deutschen Datenschutzbehörden das Videoüberwachungsverbesserungsgesetz als überflüssig ab und fassten im Rahmen des Gesetzgebungsverfahrens eine Entschließung.[5] Kernbotschaften dieser Entschließung sind: Auch ohne die ausdrückliche Abwägungsklausel können die Sicherheitsbelange von Personen, die sich in öffentlich zugänglichen Bereichen aufhalten, angemessen berücksichtigt werden. Dies geschieht auch regelmäßig, denn die Zahl der Videokameras hat sich in den vergangenen Jahren in Einkaufszentren, Freizeitanlagen und im ÖPNV erheblich erhöht. Auch ist bedenklich, dass quasi durch die Hintertür Sicherheitsaufgaben privaten Stellen übertragen werden. Für die innere Sicherheit sind die Sicherheitsbehörden zuständig, nicht Privatpersonen.

[5] 9. Nov. 2016, Kühlungsborn

Mit dem Inkrafttreten der DS-GVO kam ein weiteres rechtliches Problem hinzu. Es stellte sich die Frage, ob der nationale Gesetzgeber überhaupt für die Videoüberwachung öffentlich zugänglicher Räume durch private Stellen neben dem Art. 6 Abs. 1 Buchst. f) DS-GVO eine eigenständige Regelung wie § 6 b BDSG a. F. bzw. § 4 BDSG n. F. treffen darf. Diese Rechtsfrage wurde sehr kontrovers diskutiert. Denn nationale Regelungen neben der DS-GVO sind nur zulässig, wenn eine Öffnungsklausel als Grundlage herangezogen werden kann. In der Gesetzesbegründung zu § 4 BDSG findet sich aber kein Hinweis auf eine Öffnungsklausel. Daher sprach sich die überwiegende Mehrheit der Datenschutzbehörden von Anfang an für den Anwendungsvorrang der DS-GVO aus oder stufte den § 4 BDSG als europarechtswidrig ein. Diese Ansicht wird von weiten Teilen der rechtswissenschaftlichen Literatur geteilt.

Mittlerweile gibt es eine Entscheidung des Bundesverwaltungsgerichts (BVerwG) vom März 2019, die ebenfalls davon ausgeht, dass § 4 BDSG entgegen seinem Wortlaut nur für öffentliche Stellen des Bundes und gerade nicht für private Stellen einschlägig ist. Anlass für die Entscheidung war eine Videoüberwachung in einer Zahnarztpraxis.

In der Urteilsbegründung finden sich Ausführungen zur Anwendbarkeit des § 4 BDSG, die für die weitere Arbeit der Datenschutzbehörden wegweisend sind. So sagt das Gericht, dass die Zulässigkeitsvoraussetzungen für eine Videoüberwachung in Art. 6 Abs. 1 DS-GVO abschließend geregelt sind. Die Absätze 2 und 3 enthalten nach Ansicht der Richter begrenzte Öffnungsklauseln zugunsten der Mitgliedstaaten. Nur hierauf lassen sich daher nationale Regelungen wie § 4 BDSG stützen.

Die Erlaubnisnorm des Art. 6 Abs. 1 Satz 1 Buchst. e DS-GVO kommt für eine Datenverarbeitung durch private Stellen nicht in Betracht. Danach muss nämlich eine Datenverarbeitung erforderlich sein, um eine Aufgabe wahrzunehmen, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Eine zusätzliche Abwägung mit den Interessen der Betroffenen ist nicht vorgesehen. Daher muss, so das Gericht, die Norm restriktiv ausgelegt werden. Der Erlaubnistatbestand ist also auf behördlich oder staatlich veranlasste Datenverarbeitungsvorgänge beschränkt.

Sodann folgert das Gericht, dass die Öffnungsklauseln des Art. 6 Abs. 2 und 3 DS-GVO, die für den Erlaubnistatbestand des Art. 6 Abs. 1 Satz 1 Buchst. e gelten, Videoüberwachungen durch private Stellen nicht erfassen. Anders ausgedrückt: Nur wenn öffentliche Stellen für die Zwecke des Art. 6 Abs. 1 Satz 1 Buchst. e DS-GVO Videoüberwachung einsetzen, können die Mitgliedstaaten die Öffnungsklausel nutzen und ei-

genständige Regelungen treffen, die der DS-GVO vorgehen. Die Videoüberwachung privater Stellen ist allein an Art. 6 Abs. 1 Satz 1 Buchst. f DS-GVO zu messen, sodass § 4 BDSG nicht anwendbar ist.

Das BVerwG spricht zwar nicht von einer Europarechtswidrigkeit, meint aber eine solche. Damit ist klar: Der Bundesgesetzgeber durfte nach Ansicht des BVerwG nur für die Videoüberwachung durch Bundesbehörden den Tatbestand des § 4 BDSG formulieren, nicht aber für die durch private Stellen.

## 2.) § 14 NDSG

Wollen Landesbehörden Videoüberwachung einsetzen, so ist zunächst an die Regelungen der Landesdatenschutzgesetze zu denken. In allen 16 Bundesländern finden sich spezielle Regelungen, die der DS-GVO vorgehen. Die alten Normen vor Inkrafttreten der DS-GVO konnten mit leichten Anpassungen, insbesondere an die erhöhten Anforderungen bei den Informationspflichten, beibehalten werden.

So regelte § 25 a NDSG a. F. die Beobachtung durch Bildübertragung. Danach war die Beobachtung öffentlich zugänglicher Räume durch Bildübertragung nur zulässig, soweit sie

1. zum Schutz von Personen erforderlich ist, die der beobachtenden Stelle angehören oder diese aufsuchen, oder

2. zum Schutz von Sachen erforderlich ist, die zu der beobachtenden Stelle oder zu den Personen nach Nr. 1 gehören.

Außerdem durften keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der von der Beobachtung betroffenen Personen überwiegen.

Die neue Regelung des § 14 NDSG n. F. greift diesen Gedanken des Schutzes von Personen und Sachen als Zweck der Videoüberwachung auf, erweitert um das Hausrecht. Allerdings regelt § 14 NDSG n. F. – anders als § 25 a NDSG a. F. – die Anwendungsfälle der Videoüberwachung nicht mehr abschließend. Die Erforderlichkeit einer Videoüberwachung bestimmt sich nun allein danach, ob die Behörde diese zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe einsetzt.

Notwendig ist sowohl nach altem als auch nach neuem Recht eine Interessenabwägung im Einzelfall. Wird die Erforderlichkeit bejaht (1. Stufe), dürfen ferner keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der von der Videobeobachtung betroffenen Personen überwiegen (2. Stufe). Dieses zweistufige Prüfprogramm ist geradezu klassisch für die rechtliche Prüfung einer Videoüberwachung.

Bedauerlicherweise gehen die Neuregelungen zur Videoüberwachung wesentlich weiter als nach altem Recht. § 14 NDSG kommt einer uferlosen Generalklausel gleich. Es wäre daher theoretisch möglich, dass die öffentlichen Stellen in Niedersachsen in größerem Umfang als bisher Kameras einsetzen. Bislang lässt sich eine solche Ausweitung allerdings nicht erkennen.

Bedauerlich war es zudem, dass aus dem Gesetzentwurf in letzter Minute eine Regelung zur zeitlichen Begrenzung gespeicherter Videodaten gestrichen wurde. Es gilt damit „nur noch" der allgemeine datenschutzrechtliche Grundsatz, dass gespeicherte Daten unverzüglich zu löschen sind, sofern die Daten für die Zwecke, für die sich erhoben oder verarbeitet wurden, nicht mehr erforderlich sind. Ohne klare Vorgaben durch den Gesetzgeber besteht aber immer die latente Gefahr einer Speicherung von Daten auf Vorrat.

## 3.) § 32 NPOG

Nicht anwendbar sind die Regelungen der DS-GVO für Behörden auch, wenn sie personenbezogene Daten zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit verarbeiten. In diesen Fällen greift die zeitgleich mit der DS-GVO erlassene Richtlinie zum Schutz von personenbezogenen Daten im Bereich Justiz und Inneres (JI-Richtlinie). Diese geht der DS-GVO als speziellerer Unionsrechtsakt vor.

Für Niedersachsen finden sich die spezialgesetzlichen Regelungen zur Videoüberwachung im Gefahrenabwehrrecht. Im alten Recht, also im Niedersächsischen Gesetz über die öffentliche Sicherheit und Ordnung (Nds. SOG) war die einschlägige Norm § 32. So ist es auch im neuen Polizei- und Ordnungsbehördengesetz (NPOG). Die neuen Regelungen sind jedoch wesentlich bestimmter und konkreter gefasst. Anlass hierfür waren vor allem verfassungsrechtliche Bedenken, die das Ver-

waltungsgericht Hannover in einer Entscheidung zur Videoüberwachung durch die Polizeidirektion Hannover im Jahr 2011 geäußert hatte. Danach sei die Norm des § 32 Abs. 3 Satz 1 Nds. SOG zu unbestimmt formuliert. Das Nds. SOG wurde grundlegend überarbeitet und in diesem Zuge wurden auch die Vorschriften zur Videoüberwachung neu gefasst bzw. bisher schon praktizierte Formen der Überwachung auf eine gesicherte Rechtsgrundlage gestellt.

Im Rahmen des Gesetzgebungsverfahrens war aus datenschutzrechtlicher Sicht deutliche Kritik notwendig, unter anderem weil die Möglichkeiten der Videoüberwachung in Form der Bildaufzeichnung erweitert wurden. Nach altem Recht durften solche Aufzeichnungen nur dann angefertigt werden, wenn Straftaten von erheblicher Bedeutung im Raum standen. Jetzt kann bereits dann aufgezeichnet werden, wenn es um die Verhütung irgendeiner Straftat – und sei sie noch so gering - geht. Ob dies noch verhältnismäßig ist, darf bezweifelt werden. Positiv ist hingegen, dass das neue NPOG eine ausdrückliche Regelung für die maximale Speicherdauer von Bildaufzeichnungen vorsieht. Sie sind unverzüglich, spätestens jedoch nach sechs Wochen zu löschen, soweit sie nicht zur Verfolgung von Straftaten erforderlich oder zur Behebung einer Beweisnot unerlässlich sind. Eine Speicherung von Bilddateien auf Vorrat wird damit wirksam verhindert.

Es gab zudem noch zwei weitere erfreuliche Neuregelungen: So schafft die Vorschrift des § 32 Abs. 6 NPOG eine spezifische Rechtsgrundlage für die Überwachung des öffentlichen Verkehrsraum mittels Bildübertragung, soweit dies zur Lenkung und Leitung des Straßenverkehrs erforderlich ist. Und zweitens wurde mit § 32 Abs. 4 NPOG eine Rechtsgrundlage geschaffen, die genau bestimmt, wann und zu welchem Zweck Bodycams eingesetzt werden dürfen. Problematisch sind in diesem Zusammenhang jedoch die Regelungen in Satz 4 und 5.

Diese bestimmen, dass die Kameras auch im Bereitschaftsdienst Bilder aufzeichnen dürfen, die nach spätestens 30 Sekunden überschrieben werden, wenn die Kamera nicht eingeschaltet wird. Diese sog. Pre-Recording-Funktion soll gewährleisten, dass das Geschehen unmittelbar vor dem Einschalten der Kamera durch die Beamtin oder den Beamten ebenfalls für spätere Beweiszwecke zur Verfügung steht.

Diese Form der Datenverarbeitung erscheint verfassungsrechtlich bedenklich. Zum einen erfolgt die Datenerhebung und -speicherung ohne Kenntnis der Betroffenen. Zum anderen werden die Daten von einer Vielzahl unbescholtener Bürgerinnen und Bürger erfasst, wenn auch nur für einen kurzen Zeitraum. Im Ergebnis ist die Datenverarbeitung durch Pre-Recording als nicht unerheblicher Grundrechtseingriff zu qualifizieren. Dem steht nur der Zweck der verbesserten Beweisführung gegenüber. Ob dies tatsächlich verhältnismäßig ist, darf stark bezweifelt werden.

## Fazit

Die europäischen Regelungen, zuvorderst die DS-GVO, haben nicht dazu beigetragen, die rechtliche Komplexität in Sachen Videoüberwachung zu verringern. Das ausdifferenzierte Rechtsregime vor Inkrafttreten der DS-GVO gilt nahezu unverändert fort. Ebenso wenig hat der Bundesgesetzgeber mit dem Videoüberwachungsverbesserungsgesetz für mehr Rechtsklarheit gesorgt, im Gegenteil: Die kontroversen Diskussionen zum Anwendungsbereich des § 4 BDSG n. F. haben zunächst zur großen Verwirrung und Unsicherheit geführt. Umso erfreulicher ist es, dass die Richter des BVerwG mit ihrer Entscheidung im März 2019 hier klärende Worte gefunden haben.

Über die Autorin

**Babara Thiel**

ist Landesbeauftragte für den Datenschutz des Landes Niedersachsen

# DAME 2020: VIRTUELLES FEST DER FREUDE

Nadja Bunk

„Wir sind so geflasht! Wir können es noch gar nicht glauben. Das ist Wahnsinn, das ist großartig! Wir freuen uns riesig!"

Die Hamburger Journalisten Svea Eckert und Henning Wirtz strahlen euphorisch in die Kamera, in den Händen den transparenten DAME-Pokal und einen symbolischen Scheck mit einem Preisgeld von 3.000 Euro, der beiden nochmals deutlich macht: Sie sind die Gewinner des Datenschutz Medienpreises (DAME) 2020!



Der jährlich vergebene Datenschutz Medienpreis würdigt Medienschaffende und Kreative, die das wichtige Thema Datenschutz verständlich und informativ aufbereiten und zielgruppengenau verbreiten.

Der von Svea Eckert und Henning Wirtz eingereichte Beitrag aus dem YouTube-Format „STRG+F" von funk zeigt im Selbstversuch mit einem Amazon Echo Smart Speaker, dass das Gerät auch dann zuhört, wenn es nicht zuhören soll. Svea Eckert begibt sich in der Reportage auf die Spur ihrer eigenen Daten und deckt auf, dass die datenschutzrechtlichen Bedenken kritischer Nutzer keinesfalls unbegründet sind.

## Unboxing statt Live-Preisverleihung

Wie im vergangenen Jahr musste der Preis an die Gewinner pandemiebedingt in einem Paket zugestellt werden. Die sonst so glamouröse Preisverleihung im Rahmen der jährlich stattfindenden BvD-Verbandstage wurde nun bereits zum zweiten Mal in den digitalen Raum verlegt und fand als sogenanntes Unboxing statt.

Hierbei wurden die Preisträger gebeten, mit der Kamera festzuhalten, wie sie das Paket öffnen. Nicht nur das Hamburger Gewinner-Duo freute sich über die Sendung. Auch die zwei weiteren Nominierten packten freudestrahlend

Preise aus. Preisträger der Kategorie „Bester Beitrag Print“ wurden Hannes Munzinger und Felix Ebert mit ihrem Artikel „Wie wir uns verraten/Auf Sendung“ aus der Süddeutschen Zeitung (SZ). Eine Instagram-Story über die Dating-App Lovoo aus der „News-WG“, einem jungen Politik-Format des Bayerischen Rundfunks, ist Gewinner in der Kategorie „Bester Beitrag Social Media“. Beteiligt waren hieran Tobias Schießl, Max Osenstätter, Oliver Schnuck und Robert Schöffel.


### „Wohltuender und gut recherchierter Print-Artikel“

In ihrem SZ-Artikel beschreiben Hannes Munzinger und Felix Ebert anschaulich, welches Ausmaß der Tracking-Wahn auf dem Smartphone mittlerweile angenommen hat. Denn zahlreiche Apps erstellen in einer pausenlosen Überwachung des Nutzers ein umfassendes Profil. Der Beitrag, in dem einen Tag lang eine Freiwillige den Datenverkehr ihres Handys offenbart, liefert neben interessanten Fakten auch fachliche Zusammenhänge und erklärende Grafiken.

„In Zeiten der schnellen Unterhaltung durch kurze Videoformate ist es wohltuend, einen gut recherchierten Artikel zu lesen, der in die Tiefe geht“, begründet Stefanie Rack die Entscheidung der Jury.

### „Da ist das Ding!“

In der Instagram-Story der „News-WG“ hat ein ganzes Journalistenteam im Selbstversuch die millionenfach genutzte Dating-App Lovoo auf den Prüfstand gestellt und herausgefunden, dass durch eine Radarfunktion Standort- und Nutzerdaten öffentlich gemacht werden. „Ein toller Beitrag, der es auf jeden Fall verdient hat, in der breiten Öffentlichkeit wahrgenommen zu werden“, sagte Jury-Mitglied Sebastian Sprenger.


„Da ist das Ding! Mega!“, freut sich das Team der „News-WG“ nach dem Auspacken des DAME-Pokals mit der Aufschrift „Bester Beitrag Social Media“. „Wir hätten uns natürlich noch mehr gefreut, wenn wir den Preis vor Ort abholen und die Jury und die anderen Preisträger hätten kennenlernen können. Vielleicht können wir das ja noch einmal nachholen, da würden wir uns echt freuen!“, betont Max Osenstätter stellvertretend im Video-Call mit den mitwirkenden Journalisten.

Das Video zur virtuellen Preisverleihung können Sie unter ▶ www.datenschutzmedienpreis.de anschauen.

## Bewerberrekord zeigt: Datenschutz ist in der Gesellschaft angekommen

Insgesamt waren 49 Bewerbungen für den Datenschutz Medienpreis 2020 eingegangen – ein neuer Rekord! Darunter waren Fernsehformate, Dokumentarisches, Clips und Erklärfilme, Radiobeiträge, Songs, Social-Media-Beiträge und ganze Webseiten. Erstmals wurden auch Pressetexte zum Thema Datenschutz einbezogen. Jury-Mitglied und BvD-Vorstandsvorsitzender Thomas Spaeing erklärte: „Die Vielfalt der Einreichungen hat erneut gezeigt, dass Datenschutz erklären keineswegs langweilig und verbraucherfern ist. Die Beiträge sind unterhaltsam, geistreich, gut verständlich und oft mit nachhaltiger Erkenntnis. Das genau wollten wir erreichen: Beiträge fördern, die den Datenschutz greifbarer machen, damit das Thema im Alltag als selbstverständlich wahrgenommen und achtsam mit den persönlichen Daten umgegangen wird."

Marion Zinkeler, Geschäftsführende Vorständin der Verbraucherzentrale Bayern, war das erste Mal als Jury-Mitglied dabei. „Ich freue mich sehr, am Datenschutz Medienpreis mitarbeiten zu können. Die Auswahl an Einreichungen war sehr groß und die Beschäftigung mit dem Thema hat mir nochmals gezeigt, wie wichtig es ist gut aufzuklären und umfassend zu informieren".

## Das war die DAME-Jury 2020

**Birgit Kimmel,** *Päd. Leitung der EU-Initiative klicksafe*

**Stefanie Rack,** *Päd. Referentin der EU-Initiative klicksafe*

**Frederick Richter,** *Vorstand Stiftung Datenschutz*

**Thomas Spaeing,** *Vorstandsvorsitzender des BvD*

**Dr. Sebastian Sprenger,** *Referent der DATEV-Stiftung Zukunft*

**Barbara Thiel,** *Landesbeauftragte für den Datenschutz Niedersachsen*

**Marion Zinkeler,** *Vorständin Verbraucherzentrale Bayern*

### Über die Autorin

**Nadja Bunk**
verstärkt seit Februar 2021 das Team in der BvD-Geschäftsstelle in den Bereichen Marketing und Fundraising. Zuvor war die Kommunikationsexpertin mehrere Jahre im Agenturumfeld als Beraterin und Projektmanagerin sowie im Mittelstandsunternehmen in der Presse- und Öffentlichkeitsarbeit tätig.

Der Datenschutz Medienpreis (DAME) wird seit November 2018 von der DATEV-Stiftung Zukunft gefördert. Medienpartner ist die Medienkompetenzinitiative klicksafe.

DAME 2020 DATENSCHUTZ MEDIENPREIS

## Das sagt die Jury zu den Gewinnern

### DAME 2020 Gewinner: Svea Eckert und Henning Wirtz

***Sebastian Sprenger:*** *Die Reportage von Svea Eckert und Henning Wirtz macht transparent, wieviel Privatheit wir mit der Nutzung von Alexa und Co. tatsächlich aufgeben. Smart Speaker nehmen Inhalte auf, die wir nicht mal mit Nachbarn teilen wollen. Darüber sollte man sich ernsthaft bewusst sein. Die Reportage ist fesselnd und leistet wertvolle Aufklärungsarbeit zu einem vermeintlich smarten Alltagsgegenstand.*

***Frederick Richter:*** *Svea Eckert und Henning Wirtz verdeutlichen die Risiken und Nebenwirkungen von Smart Speakern sehr lebensnah. Welche Informationen aufgrund dieser Daten über uns bekannt werden und wie unsere Daten besser geschützt werden können – das zeigt dieser Beitrag: anschaulich, ausführlich und wertvoll.*

### Bester Beitrag Social Media: Tobias Schießl, Max Osenstätter, Oliver Schnuck und Robert Schöffel

***Barbara Thiel:*** *Der Beitrag bietet inhaltliche Tiefe und holt zugleich durch Aufmachung und Sprache die junge Zielgruppe passgenau ab. Deshalb eignet er sich hervorragend für die Sensibilisierung junger Menschen vor Missbrauchsmöglichkeiten von Standortdaten. Vielleicht wird der eine oder andere, der diesen Beitrag sieht, in Zukunft ein bisschen genauer hinschauen, welche Daten eine neue App von ihm haben möchte und was sie genau mit diesen Daten anfängt.*

***Frederick Richter:*** *Dating ohne Daten – das geht natürlich nicht. Aber Dating auf Basis von Daten soll natürlich sicher sein. Dass der Datenschutz und die Datensicherheit häufig nicht die höchste Priorität in der App-Entwicklung haben, das zeigen die Macher dieses Beitrags sehr anschaulich und sehr konkret.*

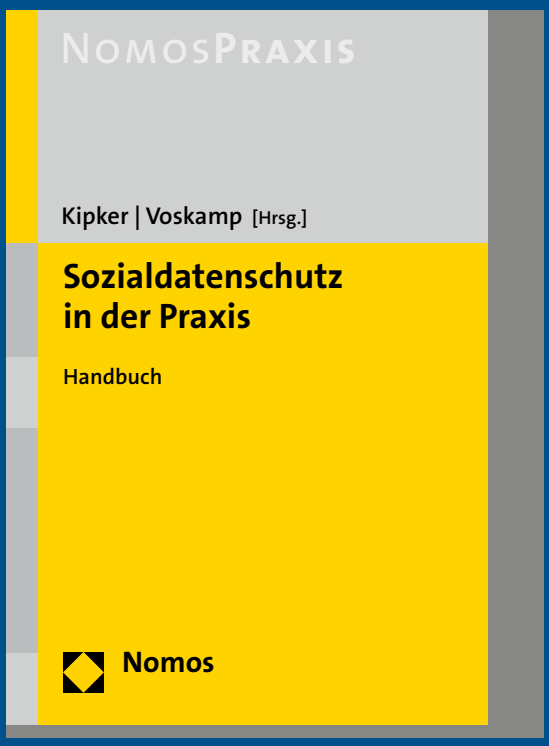
### Bester Beitrag Print: Hannes Munzinger und Felix Ebert

***Stefanie Rack:*** *Der Print-Artikel veranschaulicht in eindrucksvoller Art und Weise, wie Handydaten einer gewöhnlichen Nutzerin an einem gewöhnlichen Tag von Apps und Anbietern gesammelt und ausgewertet werden. In Zeiten der schnellen Unterhaltung durch kurze Videoformate ist es wohltuend, einen gut recherchierten Artikel zu lesen, der in die Tiefe geht.*

***Barbara Thiel:*** *Dieser Artikel aus der Süddeutschen Zeitung zeigt schonungslos, welche Dimensionen das sogenannte Tracking von Smartphone-Nutzern angenommen hat. Die Ergebnisse sind zwar leider nicht überraschend, aber trotzdem erschreckend. Der Beitrag schafft es hervorragend dieses Thema anschaulich zu machen, indem er die pausenlose Handyüberwachung an einem ganz konkreten Beispiel demonstriert.*

# SOZIALDATENSCHUTZ IN DER PRAXIS

## Dennis-Kenji Kipker, Friederike Voskamp (Hrsg.)




Dennis-Kenji Kipker, Friederike Voskamp (Hrsg.)
**»Sozialdatenschutz in der Praxis«**
**Nomos Verlag Baden Baden**

1. Auflage 2021
79,00 Euro
ISBN 978-3-8487-5843-2

Datenschutz in der Praxis? Das haben wir in den letzten Jahren oft gelesen, viele Werke wurden im Markt platziert, nach der Einführung und erst recht nach der Anwendbarkeit der Datenschutz-Grundverordnung (DSGVO) war der Bedarf riesig. Dieser wurde manches mal gut, manches Mal auch eher nicht so gut bedient. Mitunter gab es wöchentlich Neuankündigungen von neuen Werken, die Auswahl stieg schnell. Und damit insgesamt auch die Güte der Auswahl.

Aber allen diesen Werken (die mitunter mittlerweile bereits in aktualisierten Auflagen vorliegen), die dann auch tatsächlich Praxisrelevantes enthalten und nicht nur theoretisch sich dem Thema Datenschutz nach der DSGVO zuwenden, lag aber der Fokus naturgemäß auf der Grundlage des neuen europäischen Datenschutzrechts, also eben der DSGVO.

Mittlerweile hat sich dieser Markt ein wenig beruhigt und die Verlage wie auch die Autoren fangen an, über den sprichwörtlichen Tellerrand zu schauen. Der Markt öffnet sich also bereichsspezifischen Datenschutzfragen. Und genau in diese Stoßrichtung zielt das vorliegende Werk von Dennis-Kenji / Vosskamp welches konkret den Sozialdatenschutz in der Praxis zu durchdringen versucht.

Die beiden Herausgeber haben insgesamt 16 weitere Autorinnen und Autoren zu diesem Werk versammelt, von denen einige guten Gewissens als Praktiker bezeichnet werden dürfen.

Nach einer kurzen aber gut strukturierten Einführung in das Thema des Sozialdatenschutzes durch Engelke / Kipker / Vosskamp, die sich unter anderem mit der Zielsetzung, der verfassungsrechtlichen Grundlage, der sich aus der Verknüpfung mit dem Sozialrecht ergebenden Systematik des Datenschutzrechts, der Terminologie des Sozialdatenschutzrechts, den Akteuren sowie dem Verhältnis zum „normalen" allgemeinen Datenschutzrecht widmet, betrachtet das Buch in neun Kapiteln Einzelprobleme des Sozialdatenschutzes:

Beginnend mit den Betroffenenrechten und Kontrollmaßnahmen (Illner / Preuss) in Kapitel 2 (wobei hier den Betroffenenrechten deutlich Raum eingeräumt wird) folgt in Kapitel 3 Verantwortlichkeit und Zusammenarbeit (Doench / Sommerfeld). In diesem Kapitel wird sich ausführlich den möglichen rechtlichen Rahmen der Zusammenarbeit von Verantwortlichen im Sozialdatenschutz (gut gefällt eine tabellarische Übersicht am Ende diese Kapitelteils) sowie den Verschwiegenheitspflichten gewidmet.

Das vierte Kapitel (Brüggemann / Hötzel) beschäftigt sich mit dem aktuellen Themenkomplex der Digita-

lisierung, der (nicht nur durch die Politik getrieben) hochaktuell und somit in der Praxis durchaus immer öfter relevant ist. Dabei werden neben den normalen Themen wie der Kommunikation mit den Betroffenen und dem Einsatz von IT-Dienstleistern und Cloud-Diensten auch besagte aktuelle Themen wie vernetzte Medical Apps und Big Data, Telemedizin sowie elektronische Gesundheitskarte und Elektronische Patientenakte behandelt.

Kapitel 5 (Reinhardt / von Hardenberg / Marburger) arbeitet sich am Sozialverwaltungsverfahren ab: Über die Lebenszyklen der Daten von der Datenerhebung über die Speicherung, Übermittlung und Nutzung bis zu Löschung von Daten im Sozialdatenschutz.

Kapitel 6 thematisiert Datenschutz im gerichtlichen Verfahren. Hierbei fällt auf, dass auf Grund der abgeschlossenen Betrachtung der Einzelprobleme in den jeweiligen Kapiteln durchaus Doppelungen von Themen auftauchen (das Stichwort Betroffenenrechte fällt hier ins Auge). Dieses ist aber der Sache dienlich, da jeweils dem Fokus des Kapitels folgend die Themen behandelt werden und so immer wieder andere Facetten des gleichen Themas dargestellt werden können. Auch wird in diesem Kapitel auf das Thema gerichtliche Datenschutzbeauftragte eingegangen, welches sicherlich der beruflichen Tätigkeit des Kapitelautors geschuldet ist, auf jeden Fall aber interessante Einblicke in dieses Thema bietet.

Das Thema Forschung mit Sozialdaten ist eines, welches eine intensive Bearbeitung verdient und diesen Anspruch bedient das Kapitel 7 auf fast 100 Seiten. Dabei geht Kapitelautor Schäfer ausführlich auf den Sachverhalt ein. Er stellt nicht nur den rechtlichen Rahmen der Forschung dar, sondern beschreibt auch detailreich den aktuellen Stand aus der Praxis (Transparenzregeln nach den §§ 303a ff. SGB V, Forschungsdatenzentrum sowie weitere Datenquellen und Forschungsstrukturen).

Kapitel 8 und 9 behandeln die Themenkomplexe Grundsicherung für Arbeitssuchende (Schweigler) und Kinder- und Jugendhilfe (Nellissen) während das 10. Kapitel (Gode / Niemeck) sich (eher knapp) den Sozialversicherungen widmet.

## Fazit:

Dieses Werk unterstützt die praktisch im Sozialdatenschutz tätigen Personen sehr, denn bislang gab es Erkenntnisse zu dieser Thematik überwiegend nur im Zeitschriftenmarkt. Diesen gewaltigen Markt zu überblicken und nichts zu übersehen war und ist mehr als schwierig. Daher bietet das vorliegende Werk die Möglichkeit mit einem Griff in den Bücherschrank die relevanten und hilfreichen Informationen zu finden.

Die (für ein Praxishandbuch, welches das vorliegende Werk tatsächlich darstellt) eher untypische Gliederung ist logisch nachvollziehbar, der Ansatz kann gefallen. Immer wieder auftauchende Redundanzen bei bestimmten Themen helfen mehr als das sie verwirren, da sie jeweils dem Fokus des Kapitels folgend Facetten des jeweiligen Themas herausarbeiten.

Die Literaturauswahl ist (wie bei jedem Werk dieser Art) manchmal selektiv aber immer hilfreich, genauso wie die zentralen Verzeichnisse zu Stichworten, Literatur und Abkürzungen sowie die immer wieder guten Einführungen in die jeweiligen Kapitel.

Schon mit der ersten Auflage ist dem Nomos-Verlag sowie den Herausgebern und Autoren damit eine Zusammenstellung gelungen, die viele Bedürfnisse der Praxis bedient und zusätzlich auch wissenschaftliche Tiefe bietet. Ein empfehlenswertes Werk, welches der Rezensent in Zukunft gerne für die berufliche Praxis nutzen wird.

Rezension von

**Frank Spaeing**

ist externer zertifizierter Datenschutzbeauftragter (Udis), Datenschutz-Auditor (TÜV) und langjähriges, in verschiedenen Gremien aktives Mitglied im BvD

Foto: Jan Düfelsiek

# TERMINE DER REGIONALGRUPPEN UND ARBEITSKREISE DES BVD

## Die wichtigsten Daten der BvD-Gremien

**Die Arbeitskreise und Regionalgruppen sind wichtige Gremien innerhalb des BvD. Detaillierte Informationen zu den Treffen und den Terminen finden Sie unter:**

- www.bvdnet.de/regionalgruppen
- www.bvdnet.de/arbeitskreise

Die nächsten Treffen unserer Arbeitskreise und Regionalgruppen:

| | | | |
|---|---|---|---|
| **26.08.2021** | RG Nord | **22.10.2021** | RG Stuttgart |
| **09.09.2021** | RG Frankfurt | **22.10.2021** | Gemeinsames Treffen der RG München & Nürnberg |
| **16.09.2021** | AK Sozial | | |
| **17./18.09.2021** | AK Externe | **28.10.2021** | RG Nord |
| **22.09.2021** | RG Mitte | **29.10.2021** | RG Ulm |
| **23.09.2021** | RG Ost | **29.10.2021** | RG München |
| **23.09.2021** | RG Gütersloh | **23.11.2021** | RG Ost |
| **30.09.2021** | RG Nord | **25.11.2021** | RG Nord |
| **01.10.2021** | RG Karlsruhe | **25.11.2021** | RG Gütersloh |

## Bitte beachten Sie:

Aufgrund möglicher anhaltender regionaler Corona-Beschränkungen bitten wir Sie sich vorab zu informieren, welche der Termine als Präsenztreffen und welche online stattfinden.

**Sie möchten zu einem Thema aktiv mitmachen oder in Erfahrungsaustausch mit Kollegen treten?**

Termine und Anmeldung finden Sie auf unserer Webseite:

- www.bvdnet.de

**VERNETZEN SIE SICH MIT UNS:**

- www.bvdnet.de

**XING:** www.xing.com/companies/berufsverbandderdatenschutzbeauftragtendeutschlands

**TWITTER:** www.twitter.com/bvd_datenschutz

**LinkedIn:** www.linkedin.com/company/berufsverband-der-datenschutzbeauftragten

**BLOG:** www.bvdnet.de/themen/bvd-blog/

**RSS-Feed:** www.bvdnet.de/feed/

**BVD-STELLENBÖRSE**

Sie suchen ausgewiesenes Datenschutz-Knowhow für Ihr Unternehmen? Mit einer Anzeige in der BvD-Stellenbörse finden

Sie zertifizierte Datenschutzbeauftragte für eine Festanstellung oder als externe Berater. Zur Stellenbörse:

- www.bvdnet.de/bvd-stellenboerse

# WICHTIGE KONTAKTE

An dieser Stelle informiert Sie der BVD e. V. über aktuelle Kontakte zu Personen, Institutionen und Anbietern sowie wichtigen Partnern. Gerne können Sie sich hier mit Ihrem Angebot, Ihren Dienstleistungen und Ihrem Portfolio präsentieren.

Erfahren Sie mehr darüber und fordern Sie Informationen in der Geschäftsstelle unter bvd-gs@bvdnet.de an.

## Marketing

FÜR DEN BESTEN
EINDRUCK
www.tpdigitaldruck.de

**Trend Point Marketing GmbH**
Breitenbachstraße 24-29 | 13509 Berlin

## Wettbewerb

**Datenschutz Medienpreis 2021**

Bewerbungsschluss:
9. Dezember 2021

2021 DAME DATENSCHUTZ MEDIENPREIS

## Datenschutz

*Die Seminare der udis: Alles, was man zum Thema Datenschutz wissen muss.*

***Jetzt informieren unter www.udis.de***

udis zert 12345678 www.udis.de

Datenschutz geht zur Schule
BvD e.V. DATENSCHUTZ GESTALTEN

**"Datenschutz geht zur Schule" – DSgzS**
**Ein Projekt der Privacy4People gGmbH**

Budapester Straße 31 · 10787 Berlin
Telefon (030) 26 36 77 58 · Telefax (030) 26 36 77 63
dsgzs@dsgzs.de · www.dsgzs.de

privacy4people POWERED BY BvD e.V.

**privacy4people - Gesellschaft zur Förderung des Datenschutzes gGmbH**

**IHRE SPENDE FÜR DEN DATENSCHUTZ:**
Commerzbank
IBAN: DE 30 5054 0028 0424 5577 00
BIC: COBADEFFXXX

Telefon: +49 30 20 62 14 41
mail@privacy4people.de • www.privacy4people.de

*Hier könnte Ihre Anzeige stehen!*
*Jetzt Infos anfordern unter:*
*bvd-gs@bvdnet.de*

# Jetzt 3 Monate ZD kostenlos testen und Geschenk sichern!


**IHR GESCHENK**

SONDERAUSGABE DER AUSKUNFTS-ANSPRUCH NACH ART. 15 DS-GVO


## Die große Zeitschrift zum Datenschutz

Die ZD informiert umfassend über die relevanten datenschutzrechtlichen Aspekte aus allen Rechtsgebieten und begleitet die nationale sowie internationale Gesetzgebung und Diskussion um den Datenschutz. Im Mittelpunkt stehen Themen aus der Unternehmenspraxis wie z. B. ‣ Konzerndatenschutz ‣ Beschäftigtendatenschutz ‣ Datenschutz-Folgenabschätzung ‣ Compliance ‣ Kundendatenschutz ‣ Telekommunikation ‣ Soziale Netzwerke ‣ Datentransfer in Drittstaaten ‣ Vorratsdatenspeicherung ‣ Informationsfreiheit ‣ Profiling und Scoring ‣ Tracking.

## Geschaffen für die Unternehmenspraxis

Jedes Heft enthält ein Editorial, Aufsätze mit Lösungsvorschlägen, Angaben zur Lesedauer, Abstracts in Deutsch und Englisch, Schlagwortketten, Entscheidungen mit Anmerkungen und aktuelle Meldungen.

## Alles inklusive:

- Online-Modul ZDDirekt – vollständiges Online-Archiv ab ZD 1/2011
- 14-täglicher Newsdienst ZD-Aktuell
- Homepage www.zd-beck.de
- Fundstellen-Recherche in beckonline.

## 3 Hefte gratis

Bestellen Sie das kostenlose Schnupperabo unter www.beck-shop.de/go/ZD.

**ZD – Zeitschrift für Datenschutz**

11. Jahrgang. 2021. Erscheint monatlich mit 14-täglichem Newsdienst ZD-Aktuell und Online-Modul ZDDirekt.

**Jahresabonnement € 279,–**
**Vorzugspreis für BvD-Mitglieder,**
**für Abonnenten der Zeitschrift MMR und des beck-online Moduls IT- und Multimediarecht PLUS**
**sowie für ausgewählte Kooperationspartner € 219,–**

Abbestellung bis 6 Wochen vor Jahresende.
Preise inkl. MwSt., zzgl. Vertriebsgebühren € 15,– jährlich.

**beck-shop.de/go/ZD**

Erhältlich im Buchhandel oder bei: **beck-shop.de** | Verlag C.H.BECK oHG · 80791 München | kundenservice@beck.de | Preise inkl. MwSt. | 158812
facebook.com/verlagCHBECK linkedin.com/company/verlag-c-h-beck twitter.com/CHBECKRecht

C.H.BECK