EFFEKTE DER EUROPÄISCHEN DATENSCHUTZGRUNDVERORDNUNG AUF ADDITIVE MANUFACTURING

HESSEN

TECHNOLOGIELAND HESSEN

INHALT

INHALT

INHALT

Abbildungen

Tabellen

Abkürzungen

DSGVO = Europäische Datenschutzgrundverordnung
BDSG = Bundesdatenschutzgesetz
Richtlinie 95/46/EG = Europäische Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
BDSG-neu = Neufassung des Bundesdatenschutzgesetzes ab 28.05.2018
DSAnpUG-EU = Datenschutz-Anpassungs- und Umsetzungsgesetz – EU
EW = Erwägungsgrund
Art = Artikel
AF = Additive Fertigung
pb = personenbezogen (z. B. pb Daten)
DSFA = Datenschutz-Folgenabschätzung

0 EINLEITUNG

Der 25. Mai 2018 markierte das Ende der Übergangsfrist für die bereits 2016 verabschiedete Datenschutzgrundverordnung (DSGVO) der Europäischen Union. Für viele Unternehmen hatte diese Deadline einen durchaus bedrohlichen Klang. Ab diesem Tag gelten die neuen Regeln zum Datenschutz unmittelbar, also ohne weitere Rechtssetzung in allen Mitgliedstaaten der Europäischen Union – und mittelbar damit auch für alle Unternehmen weltweit, die im europäischen Binnenmarkt Geschäftsbeziehungen unterhalten, denn nach dem Marktortprinzip müssen sich alle Anbieter von Waren und Dienstleistungen an die Regeln der DSGVO halten, die in der EU niedergelassen oder tätig sind.

Die DSGVO konfrontiert Unternehmen, insbesondere KMU, mit ungewohnten Anforderungen. Viele davon sind nicht neu, besonders für deutsche Unternehmen, die einen Großteil der Regeln aus dem Bundesdatenschutzgesetz kennen. In der Vergangenheit wurde vieles davon aber durch die Datenschutzbehörden nicht geprüft oder durchgesetzt. Und neu ist jedenfalls, dass Verstöße gegen die DSGVO mit Bußgeldern bewehrt sind, die weit über bisherigen Androhungen liegen und für kleine und mittlere Unternehmen durchaus existenzgefährdende Höhen erreichen können.

Diese Studie will zweierlei leisten: Sie unterstreicht einerseits die Notwendigkeit der Einhaltung der DSGVO durch die Verantwortlichen in den Unternehmen und lenkt die Aufmerksamkeit auf die Analyse der eigenen Geschäftsprozesse, um den Handlungsbedarf bezüglich des Schutzes personenbezogener Daten zu bestimmen. Gleichzeitig betrachtet sie die Anforderungen des Datenschutzes durch die Brille einer Branche, die als produzierendes Gewerbe mit stark individualisierter Fertigung in besonderer Weise betroffen ist – nicht unbedingt stärker, aber anders als Unternehmen anderer Sektoren. In der additiven Fertigung fallen personenbezogene Daten an anderen Stellen und in anderer Weise an, als es in sonstigen verarbeitenden Industriebetrieben oder bei Dienstleistern der Fall ist. Berücksichtigt wird dabei, dass es auch innerhalb der Branche Unterschiede geben kann, abhängig zum Beispiel vom Privatkundenanteil am Geschäft, der Verarbeitungstiefe personenbezogener Daten, der Prozesssteuerung oder anderen Variablen. Implizit liefert die vorliegende Studie damit noch eine dritte Erkenntnis: Vergleichbare exemplarische Betrachtungen können für andere Branchen und Gewerbe hilfreich sein, weil sich in den spezifischen Betriebsabläufen Instanzen der Verarbeitung personenbezogener Daten zeigen können, die anderen Unternehmen völlig fremd sind.

Die ersten drei Kapitel der Studie geben – nach einer Würdigung der bisherigen Rechtslage – einen umfassenden und systematischen Überblick über neue und angepasste Regeln in Folge der DSGVO. Kapitel 4 analysiert die konkreten Voraussetzungen, betrachtet betriebliche und Prozessumgebungen und zeigt Risiken der Datenverarbeitung in Unternehmen der additiven Fertigung. Kapitel 5 gibt schließlich auf der Grundlage des ermittelten Handlungsbedarfs konkrete Empfehlungen für KMU – allgemein und speziell für Unternehmen der additiven Fertigung.

Die Furcht vor drohenden Sanktionen ist sicher kein hinreichendes Motiv, um Unternehmen zur Einhaltung des Datenschutzes zu bewegen. Genauso falsch wäre es, mögliche Verstöße und ihre Folgen für den guten Ruf der Firma oder gar eine mögliche Untersagung der Datenverarbeitung zu verharmlosen. Datenschutz soll Unternehmen nicht hemmen, sondern ihnen bei der Gestaltung ihrer Geschäftsbeziehungen behilflich sein: Er ist ein wesentlicher Baustein gelungener digitaler Transformation und kann als Alleinstellungsmerkmal die eigene Wettbewerbsfähigkeit sogar verbessern. Die DSGVO schafft grenzüberschreitende Rechtssicherheit und bildet damit die Grundlage für innovative Geschäftsmodelle. Die Anforderungen an Transparenz und Einhaltung des Rechtsrahmens gelten schon heute in vielen Geschäftsbeziehungen, gerade auch in der additiven Fertigung, wo oftmals die Regeln des Datenschutzes und der Datensicherheit bereits feste Bestandteile der Vereinbarungen mit den Auftraggebern sind.

1 ALLGEMEINE ASPEKTE VON DATENSCHUTZ UND DATENSICHERHEIT

1.1 Definition und Bedeutung

Datenschutz

Das heutige Datenschutzrecht baut auf dem juristischen Konzept des Allgemeinen Persönlichkeitsrechtes auf. Ohne dieses Recht gäbe es den Datenschutz in seiner heutigen Form nicht, denn nach der Auffassung des Bundesverfassungsgerichts ist Datenschutz ein Grundrecht – das „Recht auf informationelle Selbstbestimmung". Jeder Mensch soll grundsätzlich selbst entscheiden können, wem, wann, welche seiner persönlichen Daten zugänglich sein sollen. Dieses Recht ist jedoch nicht im Grundgesetz festgelegt, sondern wird aus anderen Grundrechten abgeleitet, insbesondere aus Art. 2 GG (allgemeines Persönlichkeitsrecht) in Verbindung mit Art. 1 GG (Menschenwürde). Bei dem Begriff „Datenschutz" geht es im juristischen Kontext demnach immer um den Schutz personenbezogener Daten. Das Datenschutzrecht dient dem Schutz vor missbräuchlicher Datenverarbeitung, des Rechts auf informationelle Selbstbestimmung, des Persönlichkeitsrechts bei der Datenverarbeitung und der Privatsphäre.

Das zentrale Motiv des Datenschutzes ist nach heutigem Verständnis der Schutz vor Datenmacht. Grundlage dafür ist die Annahme, dass der Besitz von Informationen – Daten – Machverhältnisse kreiert. Eine Datenmacht ergibt sich demnach aus einem informationellen Ungleichgewicht, welches zunächst der Staat und seit den letzten Jahrzehnten auch Unternehmen mehr und mehr gegenüber Privatpersonen gewinnen.

Geht es zwar, seit Einführung der ersten Datenschutzgesetze in der zweiten Hälfte des 20. Jahrhunderts, um den Schutz personenbezogener Daten vor Datenübermacht, haben sich die Umstände, Dimensionen und damit einhergehend auch die Bedeutung und Wichtigkeit des Datenschutzes grundlegend verändert. Zum einen sind diese Veränderungen geprägt durch die sukzessive Verschiebung von einer staatlichen Datenmacht, die zur Entwicklung des Datenschutzes geführt hat, hin zur Datenmacht von Unternehmen, die erstmals im Laufe der 1980er und 90er Jahre vermehrt als Datenverarbeiter auftauchten. Elektronische Dienste ermöglichten dann neue Dimensionen des Datensammelns. Insbesondere das Internet führte zum Aufstieg einiger mächtiger globaler Unternehmen und stellte den Datenschutz vor neue Herausforderungen. Zum anderen waren von Staat und Unternehmen gesammelte Daten im Laufe des 20. Jahrhunderts größtenteils noch analoger Natur, mit der fortschreitenden technischen Entwicklung (Stichwort „Digitale Revolution") werden seit dem Ende des 20. Jahrhunderts jedoch immer mehr Informationen digitalisiert. Dadurch können die Daten viel schneller übermittelt und verbreitet werden und sind zudem für jeden immer einfacher und schneller abrufbar.

In unserer offenen Informationsgesellschaft führt die wachsende Menge der Daten sowie die einfache Zugänglichkeit zu Kontrollverlust bezüglich der Datenverarbeitung. Vor allem ist es schwer zu kontrollieren, wie die Daten durch wen genutzt werden. Dies führt zu erheblichen Schwierigkeiten im Bestreben des Einzelnen seine Privatsphäre zu schützen und birgt Risiken in Bezug auf den Missbrauch dieser Informationen. Zudem empfinden viele Menschen zunehmend Unsicherheit und Mistrauen bei der Weitergabe persönlicher Informationen. Ein stetig angepasster Rechtsrahmen ist hier die Voraussetzung für die Wahrung des Rechts auf informationelle Selbstbestimmung. Dieser Rechtsrahmen betrifft aber nicht nur globale Unternehmen der Informationsbranche, sondern alle Unternehmen, die personenbezogene Daten verarbeiten. Der Datenschutz hat demnach mittlerweile eine übergeordnete Bedeutung in der gesamten Wirtschaft eingenommen.

Datensicherheit

Im Gegensatz zum Datenschutz, der die Theorie zum Schutz personenbezogener Daten darstellt, beschreibt der Begriff Datensicherheit die Maßnahmen, die diesbezüglich umgesetzt werden. Datenschutz ist also ohne Datensicherheit nicht möglich. Zudem betrifft die Datensicherheit alle Daten, unabhängig davon, ob diese einen Personenbezug haben oder nicht. Denn auch unternehmensbezogene Daten oder Wirtschaftsdaten bedürfen in manchen Fällen Sicherheitsmaßnahmen, denkt man zum Beispiel an Industriespionage. In Bezug auf die Einhaltung des Datenschutzes betrifft die Datensicherheit jedoch lediglich die personenbezogenen Daten.

Die Datensicherheit umfasst alle technischen und organisatorischen Maßnahmen, um folgende Aspekte in der Datenverarbeitung zu gewährleisten:

- Kontrollierbarkeit (Schutz vor Missbrauch)
- Integrität (Schutz vor Verfälschung)
- Verfügbarkeit (Schutz vor Verlust)
- Vertraulichkeit (Schutz vor unberechtigten Zugriffen)

Datensicherheit spielt insbesondere im unternehmerischen Kontext eine wichtige Rolle, da jedes datenverarbeitende Unternehmen, unabhängig von seiner Größe, gesetzlich dazu verpflichtet ist, sich mit dem Schutz personenbezogener Daten auseinanderzusetzen.

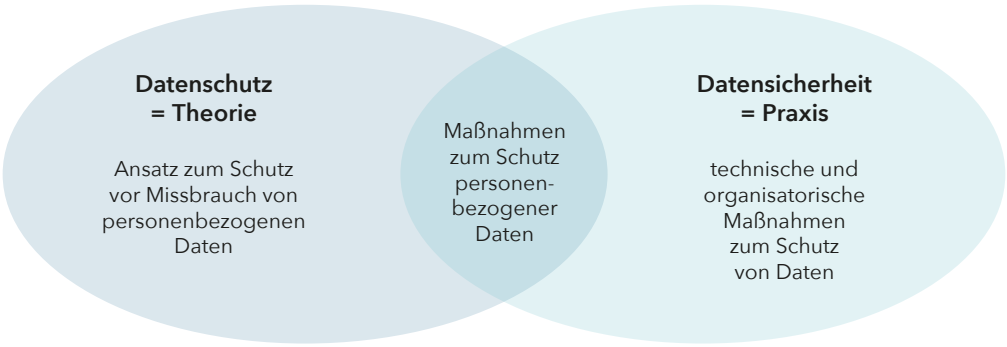


Abbildung 1: Abgrenzung Datenschutz und Datensicherheit
Quelle: Eigene Darstellung nach Brands Consulting (2017)

1.2 Exkurs: Daten

Daten sind in erkennungsfähiger Form dargestellte Elemente einer Information. Im behandelten Kontext sind Daten durch Beobachtungen, Messungen, statistische Erhebungen u. a. gewonnene Zahlenwerte oder auf Beobachtungen, Messungen, statistischen Erhebungen u. a. beruhende Angaben, formulierbare Befunde.[1]

Daten können in Systemen verarbeitet werden. Man unterscheidet dabei zwischen digitalen und analogen Daten.

Es gibt verschiedene Arten von Daten. Unterschieden werden Daten nach:

Daten können gleichzeitig unterschiedlichen Datenarten angehören, liegen aber für gewöhnlich entweder numerisch oder kategorial vor. Numerische Daten sind Sachverhalte, die durch Zahlen oder Nummern dargestellt werden. Kategoriale Daten bezeichnen dagegen Merkmale die eine begrenzte Anzahl von Ausprägungen (Kategorien) haben.

Aufbau	• Numerische Daten (Ziffern) • Alphabetische Daten (Buchstaben) • Alphanumerische Daten (Ziffern, Buchstaben und Sonderzeichen)
Beständigkeit	• Stammdaten (fest, unterliegen keiner Veränderung) • Bewegungsdaten (variabel)
Verwendungszweck	• Ordnungsdaten (ordnen, sortieren und klassifizieren) • Mengen-/Rechendaten (Angabe von Mengen)
Stellung im Verarbeitungsprozess der Datenverarbeitung	• Eingabedaten (werden zur Verarbeitung und Speicherung in eine Datenverarbeitungsanlage eingegeben, stimmen häufig mit Bewegungsdaten überein), • Gespeicherte Daten (sind schon gespeichert, stimmen häufig mit Stammdaten überein) • Ausgabedaten (Ergebnisse der Verarbeitung)

Tabelle 1: Datenklassifikation und -arten

1 Duden. (o.D.). Daten, die. Abgerufen 6. März, 2018, von https://www.duden.de/rechtschreibung/Daten

Personenbezogene Daten

Personenbezogene Daten sind ein Kernbegriff des Datenschutzes und deshalb im Kontext dieser Betrachtung besonders relevant. Daten sind personenbezogen, wenn sie eindeutig einer bestimmten natürlichen Person zugeordnet sind (identifizierte Person) oder sich der Bezug unmittelbar herstellen lässt. Liegen anonymisierte Daten vor, handelt es sich nicht um personenbezogene Daten, weil die Bezugsperson weder identifiziert noch identifizierbar ist.

Die folgende Tabelle zeigt auf, um welche Daten es sich bei personenbezogenen Daten z. B. handeln kann:

Datenkategorien	Beispiele
Allgemeine Personendaten / Personalien	Name, Geburtsort, Geburtsdatum, Nationalität, Familienstand
Adressdaten	Straße, Hausnummer, Postleitzahl, Ort
Kontaktdaten	E-Mail-Adresse, Telefonnummer, IP-Adresse
Physische Merkmale	Geschlecht, Haarfarbe, Hautfarbe, Augenfarbe, Tätowierungen, Statur, Kleidergröße, Schuhgröße
Biometrische Daten	Fingerabdruck, Gesicht, Muster der Iris
Genetische Daten	Erbliche Merkmale, genetische Probe
Gesundheitsdaten	Krankheiten, körperliche und geistige Einschränkungen, Gesundheitsdienstleitungen, psychologische Gutachten
Vorlieben	Hobbies, Vereinszugehörigkeit, sexuelle Orientierung
Überzeugungen, geistige Zustände	Einstellungen, Wünsche, politische Orientierung, Gewerkschaftszugehörigkeit, religiöse Überzeugung, ethischer Hintergrund
Besitzmerkmale	Fahrzeug- und Immobilieneigentum, Grundbucheintragungen, Kfz-Kennzeichen, Zulassungsdaten, Vermögen, Eigentum, Schulden
Kennnummern	Sozialversicherungsnummer, Steueridentifikationsnummer, Krankenversicherungsnummer, Personalausweisnummer, Matrikelnummer
Online-Daten	IP-Adressen, Standorte, besuchte Webseiten, Online-Shopping
Kaufverhalten	Produkte, Kanäle, Rückgaben, Ausgaben
Bankdaten	Kontonummern, Kreditinformationen, Kontostände
Bildung	Schul- und Universitätsabschlüsse, absolvierte Kurse
Leistung und Qualifikationen	Zeugnisse, Arbeitsleistung, Arbeitsproben /-ergebnisse, Bewertungen
Lohn und Gehalt	Höhe des Gehalts, Anzahl der Gehälter pro Jahr, Arbeitszeit (Wochenstunden), Gehaltserhöhungen
Kriminaldaten	Straftaten, Strafverfahren, Gefängnisaufenthalte
etc.	…

Tabelle 2: Personenbezogene Daten

1.3 Geschichte des Datenschutzrechts in Deutschland und der EU

Die Idee zur Notwendigkeit von Datenschutz entwickelte sich in den 1960er Jahren, in denen erstmals offenes Misstrauen gegenüber der staatlichen Datenverarbeitung aufkam. Auslöser waren strukturelle Änderungen durch den Ausbau des Sozialstaates sowie die Gliederung des Staates in verschiedene Verwaltungszweige, mit dem zu diesem Zeitpunkt bereits der Einsatz automatisierter Datenverarbeitung vorangetrieben wurde.

Im Jahr 1970 führte das Unbehagen über die wachsende staatliche Datenmacht zu den ersten Datenschutzgesetzen: Am 30. September 1970 verabschiedete Hessen als erstes Bundesland ein Landesdatenschutzgesetz. Das Gesetz regelte u. a. den Schutz elektronisch verarbeiteter Daten vor dem Zugriff Unbefugter, die Verschwiegenheit von Beschäftigten, die mit der Datenverarbeitung beauftragt sind, das Recht auf Berichtigung unrichtiger Daten sowie die Einrichtung eines Datenschutzbeauftragten für die öffentlichen Stellen. Das Gesetz führte zudem den Begriff des Datenschutzes ein.

Datenschutzgesetze in weiteren Bundesländern folgten und am 28. Januar 1977 wurde das erste entsprechende Bundesdatenschutzgesetz verabschiedet. Dies behandelte den Schutz personenbezogener Daten durch den Staat sowie auch durch Unternehmen. Eine Behörde durfte personenbezogene Daten nur dann verarbeiten, wenn dies zur Erledigung der gesetzlichen Aufgabe notwendig war, ein Gesetz dies direkt vorsah oder die Betroffenen zugestimmt hatten. In der Privatwirtschaft spielten die Vorschriften zum Datenschutz zunächst kaum eine Rolle.

Ein Meilenstein des Datenschutzes ist das Volkszählungsurteil vom 15. Dezember 1983. Eine auf den 27. April 1983 angesetzte Volkszählung hatte das Ziel, alle Einwohner Deutschlands mittels einer sogenannten Totalerhebung statistisch zu erfassen. Bürgerinitiativen riefen zum Boykott auf, nachdem ein umfangreicher Fragenkatalog veröffentlicht wurde, der laut Kritik die Identität der Befragten preisgab. Daraufhin wurde die Volkszählung ausgesetzt bis das Bundesverfassungsgericht im sogenannten „Volkszählungsurteil" das „Recht auf informationelle Selbstbestimmung" etablierte. Personenbezogene Daten dürfen seitdem durch staatliche Stellen ohne Einwilligung der Betroffenen nur dann verwendet werden, wenn dies durch ein Gesetz erlaubt wird.

Nach der Wiedervereinigung verabschiedeten auch die neuen Bundesländer in den nächsten zwei Jahren eigene Datenschutzgesetze.

Mit der Vertiefung der Europäischen Union, kam es 1995 zur ersten EU-Datenschutzrichtlinie. Sie beschreibt die Mindeststandards für den Datenschutz, die in allen Mitgliedstaaten der Europäischen Union durch nationale Gesetze sichergestellt werden müssen. In Deutschland trat zu dessen Umsetzung am 23. Mai 2001 das geänderte Bundesdatenschutzgesetz in Kraft. 2003 wurde der erste Europäische Datenschutzbeauftragte gewählt. Im Mai 2018 wurde die Richtlinie von 1995 durch die neue Europäische Datenschutzgrundverordnung zum ersten Mal abgelöst.

Nach Urteilen des Europäischen Gerichtshofes wurden in Deutschland 2009 und 2010 aufgrund einiger Datenpannen Änderungen im BDSG durchgeführt, die die Tätigkeit von Auskunfteien, das Scoring sowie den Adresshandel neu regeln. Weitere Entwicklungen des Datenschutzrechtes in den nächsten Jahren gehen ebenfalls auf die Rechtsprechung des Europäischen Gerichtshofs zurück.

Zur Modernisierung des Datenschutzrechts in Europa wurde von der EU-Kommission im Januar 2012 eine EU-Datenschutzreform vorgestellt. Nach Jahren intensiver Diskussion um die Reform des europäischen Datenschutzrechts, trat im Mai 2016 die Datenschutz-Grundverordnung (EU) 2016/679 in Kraft. Im Gegensatz zur EU-Datenschutzrichtlinie, die von den EU-Mitgliedstaaten in nationales Recht umgesetzt werden musste, ist die Datenschutzgrundverordnung ohne Umsetzungsakt in allen EU-Mitgliedsstaaten seit dem 25. Mai 2018 – zwei Jahre nach Inkrafttreten – unmittelbar anwendbar.

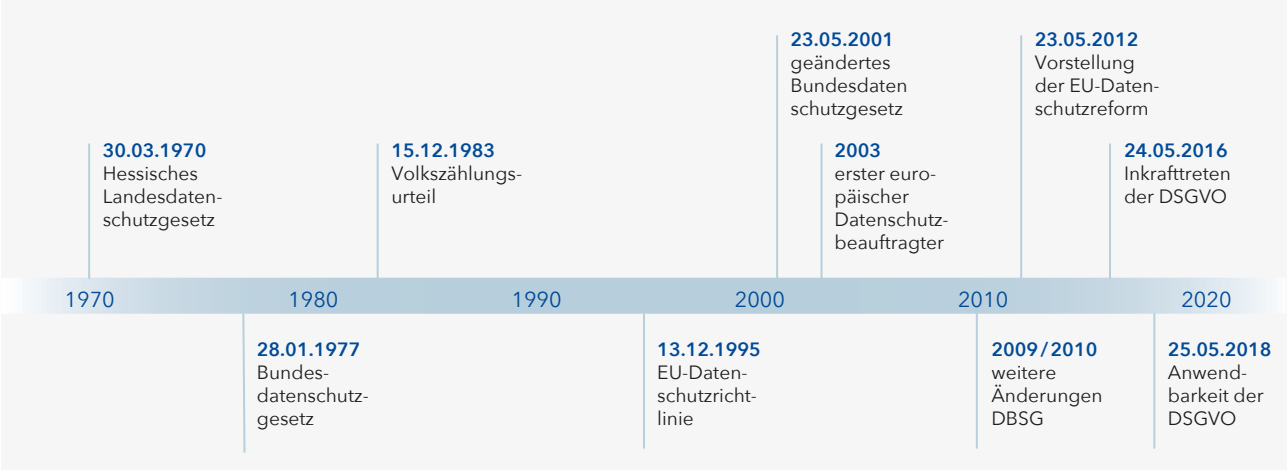


Abbildung 2: Timeline zum deutschen Datenschutzrecht
Quelle: Eigene Darstellung

1.4 Datenschutz und Datensicherheit in KMU

1.4.1 Bedeutung für KMU

Datenschutz und Datensicherheit war lange Zeit kein zentrales Thema für Unternehmen, im Gegenteil, es war selbstverständlich, dass Daten gesammelt, ausgewertet, genutzt und weiterverkauft werden konnten. Es gab zwar regulierende Gesetze, dennoch mussten Unternehmen selten Rechenschaft über die Verarbeitung der Daten ablegen. Mit Häufung der Datenschutzskandale in den 2000er Jahren durch große Unternehmen – z. B. Telekom, Lidl, Daimler, Deutsche Bahn – wurde die Datenmacht der Unternehmen immer deutlicher und die Angst vor Missbrauch stieg.

Dass im Zeitalter der Digitalisierung jedoch nicht nur große Unternehmen, sondern auch kleine und mittelständische Unternehmen der verschiedensten Branchen Daten sammeln und verarbeiten, liegt nahe und ist oft durch neue Geschäftsmodelle unvermeidlich. Insbesondere bei den KMU können dabei oft Sicherheitslücken entstehen: Den Veränderungen in Produktions- und Arbeitsprozessen durch den rasanten technischen Fortschritt und der damit verbundenen Datenverarbeitung sind kleinere Unternehmen oft nicht gewachsen, da es an Mitarbeitern mit spezifischen Kenntnissen mangelt, insbesondere im IT-Bereich. Durch die so entstehenden Sicherheitslücken sind KMU zudem vermehrt Ziel von Hacker-Angriffen. Laut einer Schätzung im Rahmen des „State of the Channel Ransomware Reports" des amerikanischen Datenanbieters Datto wurden 2017 rund fünf Prozent aller KMU weltweit[2] Opfer solcher Angriffe. Im Vergleich mit größeren Unternehmen ziehen Firmen mit weniger als 250 Mitarbeitern 43 Prozent aller Attacken[3] auf sich, deutlich mehr als ihr Anteil an den gesamtwirtschaftlichen Umsatzvolumina. Sie sind damit nicht nur exponiertere Ziele: Dass mögliche Schäden in Millionenhöhe für KMU schwerer zu verkraften sind, verschärft die Bedrohungslage.

Datenschutz und Datensicherheit wird aufgrund neuer Technologien, wachsender Datenmengen und höherer Anforderungen durch den Gesetzgeber auch für KMU einerseits zwar immer wichtiger aber andererseits auch immer schwieriger umzusetzen. Folgend sind einige wichtige Aspekte dargelegt, warum Datenschutz und Datensicherheit – unabhängig von der Angst vor Sanktionen bei Nichteinhaltung der Gesetze – auch in KMU von primärer Relevanz sein sollten:

Verantwortung
Auch KMU haben die moralische Aufgabe, die Daten, die ihnen von Kundinnen und Kunden anvertraut wurden, zu schützen – vor kriminellen Attacken, vor unbefugtem Zugriff und vor internen Datenlecks sowie vor zweckentfremdeter Nutzung. Nicht nur das Einhalten des Rechts auf informationelle Selbstbestimmung, sondern auch der Respekt vor der Privatsphäre jedes Einzelnen sollte eine Motivation sein.

Datenschutz als Wettbewerbsfaktor
Datenschutz wird in Unternehmen häufig als Hemmnis und Beschränkung aufgefasst. Durch Datenschutzverstöße und -skandale kann ein Unternehmen jedoch heute neben finanziellen Strafen auch mit einer Schädigung seines guten Rufes rechnen. Dies kann insbesondere bei KMU erheblichen Schaden anrichten, da diese auf ihre Reputation in besonderem Maße angewiesen sind. Die Beachtung datenschutzrechtlicher Bestimmungen sollte deshalb nicht als lästig empfunden werden, sondern kann vielmehr auch einen Wettbewerbsvorteil für die Unternehmen bedeuten.

2 Für die Erhebung wurden 1.700 Dienstleister befragt, die sich um die IT-Sicherheit von über 100.000 kleinen und mittleren Unternehmen weltweit kümmern.
3 Symantec. (2016). Internet Security Threat Report (Volume 21, April 2016). Abgerufen von https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf, S. 43

Dies ist ebenfalls Inhalt der Idee des „marktwirtschaftlichen Datenschutzes". Nach Auffassung dieser Theorie ist ein moderner Datenschutz nur dann umzusetzen, wenn die für die Datenverarbeitung verantwortlichen Organisationen ein eigenes Interesse an der Umsetzung datenschutzrechtlicher Vorgaben haben.

Schutz vor Internetkriminalität

„Internetkriminalität/Cybercrime umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die mittels dieser Informationstechnik begangen werden."[4]

Bei Angriffen durch Internetkriminalität besteht nicht nur das Risiko des Verlustes personenbezogener Daten, auch Unternehmensdaten können betroffen sein. Dies bedeutet zwar keine Bußgelder für das Unternehmen, kann aber in falschen Händen ebenfalls zu Datenmissbrauch führen und dem Unternehmen Wettbewerbsnachteile verschaffen.

In einer Zusatzbefragung des KfW-Mittelstandspanel 2015 wurde die Häufigkeit von IT-sicherheitsrelevanten Vorfällen nach Branchen und Größenklassen in Deutschland ermittelt: Insgesamt 30 % der Vorfälle betrafen KMU. Kleinere KMU waren dabei sogar noch häufiger von Cyberkriminalität betroffen (31 %) als größere KMU (25 %).

Auch weltweite Statistiken zeigen einen stetigen Anstieg der Cyberkriminalität durch Ransomware – das ist Malware, die einen Computer infiziert und sperrt; die Angreifer verlangen Geld dafür, ihn zu entsperren. Die Kosten, die dadurch verursacht wurden, stiegen von 325 Mio. Dollar im Jahr 2015 auf 5 Mrd. Dollar in 2017. Davon waren 301 Mio. Dollar von KMU gezahltes Lösegeld für gestohlene Daten. Trotzdem erhielten 15 % der KMU, die Lösegeld zahlten, ihre Daten nicht zurück.[5] Noch mehr Schaden als die Lösegeldforderungen richten jedoch die Ausfallzeiten der Unternehmen an. Nach einer weiteren Umfrage des Softwareanbieters Malwarebytes (2017), die ihre Ergebnisse separat für Deutschland zusammenfasst, mussten 21 % der KMU sofort nach dem Angriff ihre Geschäftstätigkeit einstellen.[6]

Mitarbeiter

Der Beschäftigtendatenschutz (oder auch Arbeitnehmerdatenschutz) wird in der EU-Datenschutz-Grundverordnung nicht eigenständig geregelt, sondern den Mitgliedstaaten anhand einer Öffnungsklausel überlassen. Die ursprünglichen Regelungen bleiben zwar überwiegend bestehen, aber die neuen Bußgelder gelten auch hier.

Zudem beeinflusst der Umgang mit dem Datenschutz in einem Unternehmen auch das Verhalten der Mitarbeiter. Einerseits schafft Datensicherheit Vertrauen, denn wenn der gesetzlich auferlegte Datenschutz und somit die Wahrung personenbezogener Daten in einem Unternehmen ernst genommen werden, so wird sich der Mitarbeiter in Bezug auf seine persönlichen Arbeitnehmerdaten bei diesem Unternehmen wohl fühlen. Besonders für KMU ist die Identifikation der Angestellten mit dem Unternehmen wichtig für die Arbeitsleistung und -atmosphäre. Andererseits wird mit verschärfter Datensicherheit auch der Datendiebstahl und -missbrauch durch Mitarbeiter verhindert, da die Hürden an Daten zu kommen größer werden und sich das Risiko entdeckt zu werden erhöht.

Eine Regelung zum Arbeitnehmerdatenschutz wurde entsprechend in das überarbeitete Bundesdatenschutzgesetz aufgenommen. Insbesondere im Hinblick auf die vielen Datenschutzskandale, bei denen Mitarbeiterdaten missbraucht wurden, ist dies ebenfalls ein wichtiger Aspekt, der im Zuge der Datensicherheit in einem Unternehmen Beachtung finden sollte.

Prozessoptimierung

Die Veränderungen in Produktions- und Arbeitsprozessen sowie die Anforderungen durch den Datenschutz erfordern teilweise kosten- und zeitintensive Maßnahmen, unter anderem auch den Einsatz neuer IT-Lösungen. Die Notwendigkeit zur Einhaltung der Gesetze kann also als Anlass betrachtet werden, überholte Systeme zu ersetzen. Wer die Chancen nutzt, seine Prozesse zu optimieren und sich mit den neusten Lösungen und Technologien auseinandersetzt, kann langfristig die Datenverarbeitung im Sinne des Datenschutzes vereinfachen und dadurch sogar Geld sparen.

4 Bundeskriminalamt. (o.D.). Internetkriminalität/Cybercrime. Abgerufen 6. März, 2018, von https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html

5 Fidelis Cybersecurity. (o.D.). Cyberkriminalität 2017 in Zahlen und Fakten. Abgerufen 17. Januar, 2018, von http://blog.wiwo.de/look-at-it/files/2017/12/Cyberkriminalit%C3%A4t2017_IG.jpg

6 Schwartz Public Relations. (2017). Zweiter jährlicher Bericht über den Stand von Ransomware. Abgerufen von http://www.schwartzpr.de/de/newsroom/Malwarebytes/Osterman%202017/Osterman_Studie_zu_Ransomware_in_deutschen_KMU.pdf

1.4.2 Datensicherheit in KMU bisher

Um Datensicherheit in einem kleinen oder mittelständischen Unternehmen gewährleisten zu können, sind verschiedene technische und organisatorische Maßnahmen möglich. Laut Zusatzbefragung des KfW-Mittelstandspanel 2015 waren die von KMU zwischen 2013 und 2015 am häufigsten durchgeführten Maßnahmen zur Verbesserung der IT-Sicherheit und des Datenschutzes folgende (Nr. 1 wurde entsprechend am häufigsten genannt):[7]

1. Einsatz entsprechender Software (z. B. Virenschutz, Firewall)
2. Erstellung und Umsetzung von Backup-Konzepten
3. Verschlüsselung von Daten, Datenträgern und E-Mail-Verkehr
4. Erstellung und Umsetzung von Berechtigungskonzepten (z. B. Passwortschutz)
5. Mitarbeiterschulungen zu Verhaltensänderungen
6. Engagement Beauftragung eines externen (unabhängigen) IT-Sicherheits-Dienstleisters
7. Bauliche Maßnahmen (z. B. Zugangskontrollen, Umzäunung, Alarmanlagen)
8. Einstellung neuer Mitarbeiter mit IT-Fachkenntnissen

Um die richtigen Maßnahmen auswählen und zielgerichtet durchführen zu können, ist ein übergreifendes Datenschutzmanagement unabdingbar (siehe auch Kapitel 5.2).

7 Schwartz, M., & Muhle, A. (2016). Chancen der Digitalisierung nutzen: Datenschutz und IT-Sicherheit gehören dazu (Nr. 117). Abgerufen von https://www.kfw.de/PDF/Download-Center/Konzernthemen/Research/PDF-Dokumente-Fokus-Volkswirtschaft/Fokus-Nr.-117-Februar-2016-Chancen-der-Digitalisierung-nutzen.pdf

2 DSGVO – HINTERGRUND UND INHALTE

2.1 Hintergrund

Überblick Entstehung und Umsetzung der DSGVO:
- Vorschlag: 25. Januar 2012
- Veröffentlichung: 4. Mai 2016
- Inkrafttreten: seit 24. Mai 2016
- Anwendung ab: 25. Mai 2018

Die erste und bis zur Ablösung der Europäischen Datenschutzgrundverordnung gültige Europäische Datenschutzrichtlinie (Richtlinie 95/46/EG) wurde 1995 erlassen und daraufhin von den Mitgliedstaaten in nationale Gesetzte umgesetzt.

Im Telekommunikationsbereich wurde die Datenschutzrichtlinie durch die im Jahr 2002 erlassene Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) ergänzt, die ebenfalls in nationales Recht umgesetzt wurde.

Durch die enormen Entwicklungen im Bereich der Erhebung, Speicherung und Nutzung personenbezogener Daten seit Mitte der 1990er Jahr war die Richtlinie 95/46/EG schnell veraltet. Die individuelle Umsetzung der Richtlinie durch die Mitgliedsstaaten hatte zudem eine heterogene Gesetzeslage in Europa zur Folge, die im Hinblick auf die zunehmende Internationalisierung zu Problemen führte. Einige Länder setzten die Datenschutzrichtlinie in vergleichsweise lockere nationale Gesetzte um, von denen große datenverarbeitende Unternehmen profitierten und als Konsequenz ihren Hauptsitz in ebendiese Länder verlegten z. B. die Google European Headquarters in Irland.

Nach zwei Konsultationsverfahren der EU-Kommission zu Datenschutz und zur Datenschutzrichtlinie sowie einem Beschluss des Europäischen Gerichtshofes vom 24.11.2011 zur Harmonisierung des Datenschutzes der EU-Mitgliedsstaaten, legte die EU-Kommission am 25.01.2012 einen umfassenden Reformvorschlag für den Datenschutz vor. Neben der Angleichung des nationalen Rechts war mehr Kontrolle für Betroffene über ihre persönlichen Daten eines der Hauptziele der Reform.

Es folgten Verhandlungen verschiedener Interessensgruppen. Die Lobbyisten der europäischen Wirtschaft waren an einem möglichst nicht regulierten Markt interessiert, während Bürgerrechtler darauf aufmerksam machten, dass die Privatsphäre ein Menschenrecht ist. Dem ausgehandelten Kompromiss (Gesetzesentwurf) stimmte im Jahr 2014 das Europäische Parlament und 2015 der Europäische Rat zu.

Die endgültige DSGVO trat im Mai 2016 in Kraft. Die DSGVO ist im Gegensatz zur Richtlinie von 1995 unmittelbar in allen Mitgliedstaaten gültig, denen jedoch eine Frist von zwei Jahren bis zur Anwendbarkeit eingeräumt wurde. Ab dem 25. Mai 2018 ersetzte die DSGVO dann nationales Recht in den Punkten, wo es im Widerspruch stand. Die in Deutschland betroffenen Gesetze sind hauptsächlich das BDSG und das Telemediengesetz (TMG), die entsprechend angepasst werden mussten. Wichtig dabei ist, dass nationale Regelungen den Datenschutz weder abschwächen noch verstärken dürfen. Allerdings enthält die Verordnung verschiedene Öffnungsklauseln, die es den Mitgliedstaaten ermöglichen, bestimmte Aspekte selbst zu regeln. Die DSGVO wird daher auch als ein „Hybrid" zwischen Richtlinie und Verordnung bezeichnet.

2.2 Konsequenzen

2.2.1 Neues Bundesdatenschutzgesetz (BDSG-neu)

Überblick Entstehung und Umsetzung

BDSG:

- Ursprüngliche Fassung: 27. Januar 1977
- Inkrafttreten: 1. Januar 1978
- Neubekanntmachung: 14. Januar 2003

BDSG-neu:

- Verabschiedung Gesetzesentwurf: 27. April 2017
- Letzte Neufassung: 30. Juni 2017
- Inkrafttreten: 25. Mai 2018

Für das nationale Recht bedeutet die DSGVO eine Anpassung des BDSG. Am 27. April 2017 hat der Bundestag den Entwurf eines neuen Bundesdatenschutzgesetzes (BDSG-neu) angenommen, welches Teil des Datenschutz-Anpassungs- und Umsetzungsgesetz – EU (DSAnpUG-EU) ist.[8] Das BSDG-neu ist mit Anwendbarkeit der DSGVO ebenfalls am 25. Mai 2018 in Kraft getreten.

Die Neufassung des BDSG besteht statt wie bisher aus 48 Paragraphen nun aus 85 Paragraphen und ist damit deutlich umfangreicher. Der Spielraum, der den nationalen Gesetzgebern durch die EU- DSGVO im Rahmen von 69 Öffnungsklauseln bleibt, wurde in der BDSG-neu an vielen Stellen genutzt. Grundsätzlich lassen sich allgemeine und spezifische Öffnungsklauseln unterscheiden. Die allgemeinen eröffnen Möglichkeiten zur Abweichung ohne auf ein Themengebiet zu beschränken, während spezifische Öffnungsklausen Abweichungen nur in einem beschränkten Bereich zulassen. Die nationalen Gesetze dürfen innerhalb dieser Klauseln die Regelungen konkretisieren, ergänzen oder sogar modifizieren.[9] Wichtige Bereiche, die durch die BSDG-neu aufgrund der Öffnungsklauseln geregelt werden sind:

- Beschäftigtendatenschutz
- Datenschutzbeauftragter
- Bußgeldbestände
- Strafvorschriften

Um zu vermeiden, dass Uneinigkeiten darüber auftreten, ob eine Regelung nun in den vorgesehenen Handlungsspielraum der jeweiligen Öffnungsklausel passt oder die nationale Regelung den Handlungsspielraum überschreitet, beinhaltet die BDSG-neu eine Klausel, die sicherstellen soll, dass keine Regelungen unzulässig in die DSGVO eingreifen:

§ 1 Abs. 5 BDSG-neu: *„Die Vorschriften dieses Gesetzes finden keine Anwendung, soweit das Recht der Europäischen Union, im Besonderen die Verordnung (EU) 2016/679 in der jeweiligen Fassung, unmittelbar gilt."*

8 https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl117s2159.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1520518907773

9 Kühling, J., Martini, M., Heberlein, J., Kühl, B., Nink, D., Weinzierl, Q., & Wenzel, M. (2016). Die Datenschutz-Grundverordnung und das nationale Recht. Abgerufen von http://www.foev-speyer.de/files/de/downloads/Kuehling_Martini_et_al_Die_DSGVO_und_das_nationale_Recht_2016.pdf

2.2.2 Konsequenzen für KMU

Unternehmen müssen seit dem 25. Mai 2018 zeitgleich sowohl die Vorgaben der DSGVO als auch des BDSG-neu umsetzen. Um sich auf die neuen Regelungen der DSGVO einzustellen, hatten sie zwei Jahre Zeit, bei der BDSG-neu war es ein knappes Jahr.

Im Vergleich zur vorherigen Rechtslage beinhaltet die Anwendung der DSGVO eine Verschärfung der bisherigen Regelungen und stellt Unternehmen vor eine Vielzahl von Herausforderungen im Hinblick auf die entsprechende Anpassung ihrer Datensicherheit. Insbesondere für kleine und mittelständische Unternehmen ergibt sich hier ein verhältnismäßig großer Aufwand, der sich in zusätzlichen Kosten für technische Lösungen (IT-Sicherheitssysteme), Personal, Dienstleitungen etc. niederschlägt. Die konkreten Änderungen, die sich durch die DSGVO im Vergleich zur BDSG ergeben und die daraus folgenden Anforderungen für KMU werden in Kapitel 3 ausführlich betrachtet.

Bei der Suche nach der optimalen Lösung werden weitere Hindernisse deutlich. Die DSGVO und das BDSG-neu sind nebeneinander anzuwenden, Unternehmen müssen ihre Datensicherheit demnach so anpassen, dass sie beiden Vorschriften genügen. Das komplexe Zusammenspiel zwischen DSGVO und BDSG-neu ist jedoch für Nicht-Juristen schwer zu interpretieren und zu verstehen – das stellt KMU vor besondere Herausforderungen, da sie in der Regel nicht über eigenes juristisch ausgebildetes Personal verfügen, welches sich mit der Thematik auseinandersetzen kann.

So ist es nicht verwunderlich, dass zunächst bei Inkrafttreten der DSGVO und erneut bei der Verabschiedung des BDSG-neu im April 2017 vermehrt Kritik aufkam, dass die Umsetzung innerhalb eines Jahres für viele KMU kaum möglich sein wird.

2.3 Inhalte der DSGVO

2.3.1 Struktur

Die Europäische Datenschutzgrundverordnung setzt sich aus 99 Artikeln zusammen, die sich auf 11 Kapitel verteilen. Dem sind 173 Erwägungsgründe (EW) vorangestellt, die den Artikeln zugeordnet sind. Die Erwägungsgründe beinhalten, je nach Betrachtungswinkel, die Herleitung zu den Artikeln oder geben eine Erklärung zu Inhalt und Zweck des jeweiligen Artikels.

In der nebenstehendenTabelle sind Aufbau und Inhalte der DSGVO zusammengefasst dargestellt.

Die Europäische Datenschutzgrundverordnung steht auf dem Online-Portal EUR-Lex[10] in allen 24 Sprachen der Europäischen Union zum Download zur Verfügung.

10 Siehe: http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679

Kap.	Titel	Inhalte	Artikel	Erwägungs-gründe
I	Allgemeine Bestimmungen	• Erläuterung und Eingrenzung von Anwendungs-bereich und Begrifflichkeiten	1 – 4	1 – 37
II	Grundsätze	• Wesentliche zu berücksichtigenden datenschutz-rechtlichen Grundsätze • Zulässigkeitsvoraussetzungen einer jeglichen Datenverarbeitung	5 – 11	38 – 57
II	Rechte der betroffe-nen Personen	• Allgemeiner Transparenzgrundsätze • Spezifische informatorische Pflichten der Verantwortlichen • Rechte der von der Datenverarbeitung Betroffenen	12 – 23	58 – 73
IV	Für die Datenverar-beitung Verantwort-liche und Auftrags-verarbeiter	• Allgemeine Verantwortlichkeiten der Daten-erheber • Spezifische Anforderungen und Grundsätze für die Konstellationen der gemeinsamen Verant-wortlichkeit, der Verantwortlichenvertretung bei Sitz des Verantwortlichen im EU-Ausland und der Auftragsdatenverarbeitung • Dokumentations- und Meldepflichten der Verantwortlichen • Stellung und Pflichten zur Benennung von Datenschutzbeauftragten	24 – 43	74 – 100
V	Übermittlung perso-nenbezogener Daten an Drittländer oder an internationale Organi-sationen	• Grundsätze und rechtlichen Anforderungen der Übermittlung von personenbezogenen Daten an Drittländer und internationale Organisationen	44 – 50	101 – 116
VI	Unabhängigkeit der Aufsichtsbehörden	• Stellung und Funktionsweise der einzurichten-den datenschutzrechtlichen Aufsichtsbehörden	51 – 59	117 – 129
VII	Zusammenarbeit und Kohärenz	• Leitlinien einer Zusammenarbeit der einzu-richtenden datenschutzrechtlichen Aufsichts-behörden	60 – 76	130 – 140
VIII	Rechtsbehelfe, Haftung und Sanktionen	• Gerichtliche und außergerichtliche Rechts-behelfe und Mittel der Betroffenen bei Verstößen gegen die Datenschutzvorgaben der Verordnung • Haftungsmaßstäbe und Sanktionen für Verant-wortliche	77 – 84	141 – 152
IX	Vorschriften für be-sondere Datenverar-beitungssituationen	• Vorschriften für besondere Verarbeitungssitua-tionen (Informationsfreiheit, Arbeitsverhältnisse, Forschung etc.)	85 – 91	153 – 165
X	Delegierte Rechtsakte und Durchführungs-rechtsakte	• Befugnisse und Bestimmungen zur Ausübung delegierte Rechtsakte und Durchführungs-rechtsakte im Ausschussverfahren	92 – 93	166 – 170
XI	Schlussbestimmungen	• Allgemeine Bestimmungen zu Aufhebung, Verhältnissen, Berichtswesen, Inkrafttreten und Anwendung der Richtlinie	94 – 99	171 – 173

Tabelle 3: Struktur und Inhalte der DSGVO
Quelle: Eigene Darstellung

2.3.2 Relevante Begriffe und Erklärungen

Die Basis für das Verständnis der DSGVO ist die unmissverständliche Klärung von Begrifflichkeiten sowie die Erläuterung grundsätzlicher Aspekte, die ein Unternehmen kennen sollte, wenn es sich mit der Umsetzung der Anforderungen der Verordnung beschäftigt.

Personenbezogene Daten
„Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind." (Art. 4)

Erläuterungen:
- Informationen die direkt auf eine Person bezogen sind, weil sie dieser zugeordnet sind oder die von der betroffenen Person selbst gemacht wurden.
- Alternativ genügt es, wenn die betroffene Person zumindest mittelbar identifizierbar ist (es ist nicht sofort offensichtlich, auf wen sich die Angaben beziehen, aber mit Hilfe von Zusatzwissen kann die Person ausfindig gemacht werden).

(Daten)Verarbeitung
„Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung." (Art. 4)

Erläuterungen:
- Automatisierte Verarbeitung: mithilfe von IT-Systemen
- Nicht automatisierte Verarbeitung: nicht mit IT-Systemen z. B. Personalakten in Papierform

Zweckdienlichkeit
„Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;(…) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung")." (Art. 5)

Erläuterungen:
- Die Zwecke der Datenverarbeitung müssen zum Zeitpunkt der Erhebung der personenbezogenen Daten festgelegt eindeutig formuliert und rechtmäßig sein.

Rechtmäßigkeit
Dieser Punkt hat besondere Relevanz, da er sich mit der Frage beschäftigt, wann Daten überhaupt zulässig verarbeitet werden dürfen.

„Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:" (Art. 6)

a) Bei Einwilligung der betroffenen Person für einen oder mehrere Zwecke
b) Zur Vertragserfüllung, einschließlich vorvertraglicher Aktivitäten (hier sind auch mündliche Verträge gemeint)
c) Zur Erfüllung einer rechtlichen Verpflichtung (z. B. Aufbewahrungspflichten von Unterlagen)
d) Um lebenswichtige Interessen von Personen schützen (z. B. im medizinischen Bereich aber auch hier sehr selten, da die meisten Fälle unter b) einzuordnen sind)
e) Zur Wahrnehmung einer Aufgabe / Pflicht des öffentlichen Interesses (wichtig für die öffentliche Hand, für Unternehmen eher irrelevant)
f) Zur Wahrung der Interessen des Verantwortlichen oder eines Dritten solange nicht die Interessen, Grundrechte und Grundfreiheiten überwiegen, insbesondere bei Kindern

Erläuterungen:
- Von den sechs Zulässigkeitstatbeständen sind drei relevant im Unternehmenskontext: a), b), f)
- Art. 6 Abs. 1 lit. f) DSGVO fordert u. a. eine Abwägung zwischen den Interessen der Betroffenen einerseits und den Interessen der Datenverarbeiter andererseits. Eine Berechtigung zur Datenverarbeitung ergibt sich nur, wenn die Interessen der Datenverarbeiter die Interessen der Betroffenen überwiegen.

2.3.3 Der Umgang mit KMU

KMU haben eine besondere Rolle in der DSGVO und erfahren eine Behandlung, bei denen ihre speziellen Bedürfnisse an manchen Stellen besonders berücksichtigt werden.

Die DSGVO betrachtet KMU innerhalb der „Kleinstunternehmen sowie kleinen und mittleren Unternehmen". Für die genaue Definition ist die Empfehlung der Kommission vom 6. Mai 2003[11] maßgeblich (siehe Erwägungsgrund (EW) 13). Darin wird folgendes festgelegt:

- Kleinstunternehmen sind Unternehmen, die weniger als 10 Mitarbeiter und einen Jahresumsatz oder eine Jahresbilanzsumme von höchstens 2 Mio. EUR haben.
- Kleine Unternehmen sind Unternehmen, die weniger als 50 Mitarbeiter und einen Jahresumsatz oder eine Jahresbilanzsumme von höchstens 10 Mio. EUR haben.
- Mittlere Unternehmen sind Unternehmen, die weniger als 250 Mitarbeiter und einen Jahresumsatz von höchstens 50 Mio. EUR oder eine Jahresbilanzsumme von höchstens 43 Mio. EUR haben.

Im folgenden Abschnitt werden die wichtigsten Inhalte der Verordnung aufgeführt, die Aufschluss über den spezifischen Umgang mit Kleinstunternehmen sowie kleinen und mittleren Unternehmen (KMU) geben. Zu beachten ist hier der Unterschied zwischen Erwägungsgründen und Artikeln, da die Erwägungsgründe nur Erläuterungen sind, die darstellen sollen, welche Überlegungen zum Erlass des Rechtsakts geführt haben, während die Artikel diesem Rechtsakt angehören.

11 Europäische Kommission. (2003). Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (2003/361/EG). Abgerufen von http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32003H0361&from=DE

Thema	relevanter Inhalt für KMU	Verweis
Berücksichtigung von Kleinstunternehmen sowie kleinen und mittleren Unternehmen	Notwendigkeit einer Verordnung, die alle Wirtschaftsteilnehmer einschließlich KMU gleichbehandelt, zum Erfüllen ihrer Zwecke – ein gleichmäßiges Datenschutzniveau für Personen und den freien Verkehr personenbezogener Daten im Binnenmarkt. Die Verordnung sollte eine abweichende Regelung hinsichtlich des Führens eines Verzeichnisses für Einrichtungen mit weniger als 250 Mitarbeitern beinhalten. Die Organe der EU, die Mitgliedstaaten und Aufsichtsbehörden werden dazu angehalten, die besonderen Bedürfnisse von KMU zu berücksichtigen. Empfehlung zur Definition von KMU (Kommission, 2003)	EW 13
Erstellung von Verhaltensregeln durch Verbände und Vereinigungen	Bestimmte Kategorien von Verbänden und Vereinigungen sollten mithilfe der Verordnung zum Ausarbeiten von Verhaltensregeln ermutigt werden, bei denen die besonderen Bedürfnisse von KMU zu berücksichtigen sind.	EW 98
Sensibilisierungsmaßnahmen und spezifische Maßnahmen	Sensibilisierungsmaßnahmen der Aufsichtsbehörden sollten spezifische Maßnahmen einschließen, die sich u. a. speziell an Kleinstunternehmen sowie kleine und mittlerer Unternehmen richten.	EW 132
Durchführungsbefugnisse der Kommission	Im Rahmen der Übertragung von Durchführungsbefugnissen auf die Kommission, sollte diese besondere Maßnahmen für Kleinstunternehmen sowie kleine und mittlere Unternehmen erwägen.	EW 167
Verzeichnis von Verarbeitungstätigkeiten	Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, müssen die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten nicht umsetzen, sofern die Verarbeitung kein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder die Verarbeitung keine besonderen Datenkategorien oder personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten einschließt.	Art. 30
Verhaltensregeln	Die Ausarbeitung von Verhaltensregeln, die zur ordnungsgemäßen Anwendung der Verordnung beitragen sollen und u. a. den besonderen Bedürfnissen von KMU Rechnung getragen wird, wird gefördert.	Art. 40
Zertifizierung	Bei der Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, wird den besonderen Bedürfnissen von KMU Rechnung getragen.	Art. 42

Tabelle 4: KMU in der DSGVO
Quelle: Eigene Darstellung

Obwohl einige Zugeständnisse an KMU gemacht wurden, gilt die DSGVO grundsätzlich für alle Organisationen, die personenbezogene Daten verarbeiten. Die Auswirkungen der DSGVO auf ein Unternehmen hängen demnach in erster Linie von der Art und Weise ab, wie Daten verarbeitet werden und nicht von der Anzahl der verarbeiteten Datensätze oder der Größe des Unternehmens.

3 DSGVO – ÄNDERUNGEN HINSICHTLICH DES BDSG UND SICH DARAUS ERGEBENDE HERAUSFORDERUNGEN FÜR KMU

Der mit der EG-Datenschutzrichtlinie verfolgte Zweck, auf europäischer Ebene einen Harmonisierungseffekt zu erreichen, realisierte sich nicht, sodass der Datenschutz in der EU nun durch eine allgemein und unmittelbar geltende Verordnung, nämlich der DSGVO geregelt wird. Auch wenn die DSGVO weiterhin einige Öffnungsklauseln enthält, die entsprechende Regulierungen von den Mitgliedstaaten gestattet, wird die DSGVO als „Basisregelung" für eine größere Harmonisierung innerhalb der EU sorgen.

Das europäische Datenschutzrecht hat Anwendungsvorrang vor dem nationalen Datenschutzrecht der Mitgliedstaaten. Dieser Anwendungsvorrang gilt allerdings nur innerhalb der Normsetzungszuständigkeiten der EU. Und soweit das europäische Datenschutzrecht den Mitgliedstaaten Ausgestaltungs- und Regelungsspielraum einräumt, können ebenfalls eigenständige Regelungen geschaffen werden.[12] Das BDSG-neu muss also nunmehr die in der DSGVO kodifizierten Prinzipien in das deutsche Recht übersetzen und zudem im Rahmen der in der DSGVO vorgegebenen Öffnungsklauseln entsprechende nationale Regelungen formulieren.

Auch wenn die DSGVO von vielen Kommentatoren als „Schreckgespenst" dargestellt wurde, ist festzuhalten, dass die DSGVO das in Deutschland geltende Datenschutzrecht nicht grundlegend verändert. Den Betroffenen wird bereits mit dem BDSG ein relativ hohes Schutzniveau im Hinblick auf ihre personenbezogenen Daten geboten.

Doch auch wenn eine Vielzahl von Regelungen schon im Rahmen des BDSG von Unternehmen zu beachten waren, heißt das nicht, dass die Unternehmen sich entspannt zurücklehnen können. Im Gegenteil: Jedes zweite Unternehmen sieht selbst bei seinem Sicherheitsniveau noch Nachbesserungsbedarf.[13] Insbesondere im Hinblick auf den drastisch erhöhten Bußgeldrahmen, den die DSGVO vorsieht, ist jedes Unternehmen gut beraten, dem Datenschutz einen entsprechenden Stellenwert einzuräumen und sowohl die bisher geltenden Vorgaben als auch die neu hinzukommenden Pflichten umzusetzen.

Die zentralen Themen der DSGVO sind vor allem die Rechtsgrundlagen der Datenverarbeitung, die Rechte der Betroffenen und die Pflichten der Verantwortlichen.

3.1 Anwendungsbereich

Soweit keine personenbezogenen Daten betroffen sind, findet die DSGVO keine Anwendung. Die Definition der personenbezogenen Daten ist allerdings sehr weit gefasst: Es reicht, wenn die Daten (Informationen) einer bestimmten Person lediglich irgendwie zugeordnet werden können und damit ein Bezug zu der betroffenen Person hergestellt werden kann (vgl. Kapitel 2.3.2).

In Art. 2 Abs. 1 DSGVO ist der sachliche Anwendungsbereich der DSGVO definiert. Danach findet die Verordnung Anwendung auf die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie auf die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Neu ist hierbei, dass der Anwendungsbereich im Hinblick auf Unternehmen auch auf die nicht automatisierte Verarbeitung ausgeweitet wurde.

Eine automatisierte Verarbeitung erfolgt z. B. unter Einsatz von Computern, Smartphones, Kameras, Webcams, Scannern oder Kopierern. Jede Computer-, Internet- und E-Mail-Nutzung kann also in den Anwendungsbereich der DSGVO fallen, wenn personenbezogene Daten betroffen sind.

Eine nicht automatisierte (manuelle) Verarbeitung von Daten liegt dagegen z. B. bei handschriftlichen Notizen vor. Voraussetzung für die Anwendbarkeit der DSGVO ist bei einer nicht automatisierten Datenverarbeitung jedoch, dass die Daten in einem Dateisystem gespeichert sind oder werden sollen. Ein Dateisystem in diesem Sinne liegt gemäß dem Erwägungsgrund 15 vor, wenn eine Ordnung der Daten nach bestimmten Kriterien erfolgt.

12 Eßer, M., Kramer, P. & Lewinski, K. V. (2017). DSGVO BDSG (5. Aufl.). Carl Heymanns Verlag.

13 Schwartz & Muhle (2016).

3.2 Betroffenenrechte

Die Rechte der Betroffenen werden insbesondere durch die in der DSGVO hinzugekommenen Transparenz- und Informationspflichten der datenverarbeitenden Stellen gestärkt. Dadurch sollen die Betroffenen leichter Zugang zu ihren Daten und über deren Nutzung erhalten.[14] Jeder Betroffene hat das Recht, zu erfahren, welche Daten über ihn gesammelt werden sowie in klarer und leicht verständlicher Form darüber informiert zu werden, wer seine Daten wie und wo und zu welchem Zweck verarbeitet. Zusätzlich hat jeder Betroffene das Recht auf Datenportabilität, d. h. seine Daten in einem „strukturierten, gängigen und maschinenlesbaren Format" zu erhalten und diese einem anderen Anbieter zu übermitteln.

Zudem wurde nun auch das „Recht auf Vergessenwerden" normiert. Das umfasst zum einen das Recht auf Löschung der eigenen Daten und zum anderen das Recht auf Berichtigung. Danach kann der Betroffene verlangen, dass unrichtige personenbezogene Daten berichtigt werden und unvollständige Daten vervollständigt werden.

3.3 Dokumentation

Durch die DSGVO kommt der Dokumentation nun eine größere Bedeutung zu.[15] Bisher galt das Prinzip, dass die Aufsichtsbehörden einen Verstoß gegen datenschutzrechtliche Vorgaben belegen mussten. Die DSGVO sieht demgegenüber jetzt eine **Rechenschaftspflicht** vor, in dem sie normiert, dass der Datenverarbeiter (Verantwortliche) für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich ist und ihre Einhaltung nachweisen kann (Art. 5 Abs. 2 DSGVO). Die Nachweispflicht bezieht sich explizit auf die gesamte DSGVO und umfasst auch die in Art. 5 DSGVO niedergelegten Grundsätze Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung Integrität und Vertraulichkeit.

Darüber hinaus ist an dieser Stelle weiterhin das **Verzeichnis von Verarbeitungstätigkeiten** zu nennen. Wie bereits im BDSG vorgeschrieben, ist der Verantwortliche verpflichtet, eine Dokumentation über alle Verfahren zu erstellen, bei denen personenbezogene Daten verarbeitet werden. In bestimmten Grenzen sind gem. Art. 30 Abs. 5 DSGVO Ausnahmen von dieser Verpflichtung möglich für Unternehmen mit weniger als 250 Mitarbeitern.

Der tatsächliche Anwendungsbereich dieser Ausnahmeregelung wird allerdings marginal sein. Auch wenn in der Literatur teilweise die Ansicht vertreten wird, dass der Erwägungsgrund 13 dafür spräche, dass die in Art. 30 Abs. 5 DSGVO enthaltene Ausnahmeregelung weit auszulegen sei, gehen die unabhängigen Datenschutzbehörden des Bundes und der Länder von einer engen Auslegung aus.[16]

Die DSGVO schreibt vor, dass in das Verzeichnis im Vergleich zum Verfahrensverzeichnis nach dem BDSG ergänzende Angaben aufzunehmen sind, so z. B. die Kontaktdaten eines bestellten Datenschutzbeauftragten, Löschfristen und eine allgemeine Beschreibung der technisch-organisatorischen Maßnahmen. Auf Anfrage ist das Verzeichnis der Aufsichtsbehörde zur Verfügung zu stellen. Das bisher im BDSG geregelte Verzeichnis für jedermann fällt dafür weg.

14 Solmecke, C. (o.D.). Die EU-Datenschutzgrundverordnung – was ändert sich 2018? Abgerufen 6. März, 2018, von https://www.wbs-law.de/it-recht/datenschutzrecht/die-eu-datenschutzgrundverordnung/

15 Lepperhoff, N., & Müthlein, T. (2017). Leitfaden zur Datenschutz-Grundverordnung. Zwickau: Datakontext. S. 65 ff.

16 Unabhängige Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK). (2017). Kurzpapier Nr. 1 Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO. Abgerufen von https://www.datenschutzzentrum.de/artikel/1159-.html

3.4 Auftragsdatenverarbeitung

In der Auftragsdatenverarbeitung ist neu, dass jetzt auch die Stellen, die personenbezogene Daten weisungsgebunden für den Verantwortlichen verarbeiten (Auftragsverarbeiter) unmittelbar mit Pflichten belegt werden.[17] Gravierend ist dabei, dass auch der Auftragsverarbeiter nunmehr als Verantwortlicher für eine unautorisierte Verarbeitung zur Rechenschaft gezogen werden kann und für einen infolge rechtswidriger Datenverarbeitung eingetretenen materiellen oder immateriellen Schaden haften muss (Art. 82 Abs. 1 DSGVO).[18]

Zukünftig werden auch mehrere Stellen eine erlaubte Datenverarbeitung gemeinsam durchführen können. Dies erfordert eine transparente Vereinbarung, in der die Zwecke der Verarbeitung und die Verantwortlichkeiten sowie die Handhabung bezüglich der Betroffenenrechte geregelt werden.

Alle bisher zur Auftragsdatenverarbeitung geschlossenen Verträge müssen an das neue Recht der DSGVO angepasst werden. Dies bedeutet für die KMU, dass sie alle Auftrags(daten)verarbeiter identifizieren müssen. Gerade kleineren Unternehmen, die bisher noch keine großen Berührungspunkte zum Datenschutz hatten, wird dies unter Umständen schwerfallen. So fallen z. B. auch Reinigungsunternehmen und Wartungsunternehmen für Kopierer (mit Festplatte) unter den Tatbestand der Auftragsverarbeitung, was auf den ersten Blick nicht sofort erkennbar ist.

Sofern ein KMU selbst als Dienstleister und Auftragsverarbeiter fungiert, sind die Änderungen maßgeblicher Natur. Der Auftragsverarbeiter steht grundsätzlich in einer gemeinsamen, gesamtschuldnerischen Haftung mit dem Auftraggeber gegenüber dem Betroffenen.

3.5 Datenschutz-Folgenabschätzung

Jedem Unternehmen obliegt nach der DSGVO die Pflicht, eine Datenschutz-Folgenabschätzung (DSFA) vorzunehmen und entsprechende notwendige Schutzmaßnahmen zu etablieren, wenn ein Datenverarbeitungsverfahren voraussichtlich ein hohes Risiko für die Rechte und Freiheiten des Betroffenen birgt.

Die DSFA erfolgt in drei Schritten:

1. Zunächst ist eine Risikoanalyse vorzunehmen.

2. Wenn die Analyse ein hohes Risiko statuiert, ist eine DSFA zu erstellen, in deren Rahmen auch die technischen, organisatorischen und rechtlichen Maßnahmen zu beschreiben sind, die das Risiko minimieren.

3. Verbleibt danach immer noch ein (restliches) hohes Risiko, dann ist die zuständige Aufsichtsbehörde zu informieren.[19]

Das bedeutet in der Praxis, dass für den Einsatz der Anwendung vorab eine Genehmigung der zuständigen Datenschutzaufsichtsbehörde einzuholen ist, wenn sich ein hohes oder sehr hohes Risiko nicht durch angemessene technische und / oder organisatorische Maßnahmen reduzieren lässt.

17 Lepperhoff & Müthlein (2017), Ziffer 1.2.3.2
18 Lepperhoff & Müthlein (2017), Ziffer 1.2.3.2

19 Brockhausen, C. (2017, 4. September). Datenschutz: Das optimale „Privacy Impact Assessment" nach der DSGVO. Compliance Praxis, 19(3). Abgerufen von http://www.compliance-praxis.at/Fachartikel/Datenschutz-Das-optimale-Privacy-Impact-Assessment-nach-der-DSGVO/(shareHash)/9dbeb0f273f311c05dae24e179df8e1c

Abbildung 3: Datenschutzfolgenabschätzung
Quelle: Eigene Darstellung nach Datenschutzkonferenz (2017) [20]

3.6 Technische und organisatorische Maßnahmen

Mit Art. 32 DSGVO wurden die Verpflichtungen neu definiert, ein angemessenes Schutzniveau durch die Implementierung geeigneter technischer und organisatorischer Maßnahmen (TOM) zu gewährleisten. Dabei sollen der Stand der Technik, die Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die Eintrittswahrscheinlichkeit und Schwere des Risikos berücksichtigt werden. Die Schutzziele der IT-Sicherheit gelten unter der DSGVO als zentrale Elemente, wenn es darum geht, unter dem Aspekt des Datenschutzes die Sicherheit der Verarbeitung zu gewährleisten. Die Schutzziele sind:

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Zudem kamen folgende neue Anforderungen an TOM hinzu:

Privacy by Design (Datenschutz durch Technikgestaltung) bedeutet, dass bereits bei der Planung und Entwicklung von IT-Systemen die Ziele des Datenschutzes und der Datensicherheit zu berücksichtigen sind, mit der Intention, dass die Datenverarbeitungsprozesse schon von vornherein datenschutzfreundlich sind.

Neu ist darüber hinaus auch die Pflicht, elektronische Geräte und Anwendungen datenschutzfreundlich voreinzustellen, d.h., dass nur solche Daten erhoben werden, die für den Zweck der Verarbeitung benötigt werden.[21] Dieses Prinzip wird **Privacy by Default** (datenschutzfreundliche Voreinstellungen) genannt.

20 Unabhängige Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK). (2017). Kurzpapier Nr. 5: Daten-schutz-Folgenabschätzung nach Art. 35 DS-GVO. Abgerufen von https://www.datenschutzzentrum.de/artikel/1162-.html

21 Solmecke (o.D.)

3.7 Meldepflicht

Die bisher im BDSG normierte Meldepflicht bei Datenpannen ist ebenfalls modifiziert worden. Die DSGVO sieht in Art. 33 vor, dass grundsätzlich alle Verletzungen binnen 72 Stunden an die Aufsichtsbehörde zu melden sind. Dabei müssen die folgenden Informationen mitgeteilt werden:

- Beschreibung der Datenpanne unter Angabe der Datenkategorie, der Anzahl der betroffenen Personen und der Anzahl der betroffenen Datensätze
- Kontaktdaten des Datenschutzbeauftragten
- Eine Beschreibung der Folgen aus der Datenpanne
- Eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenpanne und zur Abmilderung ihrer Folgen.

Die Meldepflicht beschränkt sich nunmehr nicht mehr nur auf die unrechtmäßige Kenntnisnahme durch Dritte. Auch die Vernichtung, der Verlust und eine Veränderung der Daten muss u. a. angezeigt werden. Zudem wurde die Unterscheidung zwischen Risiko- und sonstigen Daten aufgegeben. Die Meldepflicht nach der DSGVO betrifft alle personenbezogenen Daten. Das führt dazu, dass selbst die unbefugte interne Weitergabe als Schutzverletzung angesehen werden kann.[22]

Darüber hinaus ist gem. Art 34 Abs. 5 DSGVO auch der Betroffene von der Datenpanne zu unterrichten, sofern diese mit einem „hohen Risiko" für die persönlichen Rechte und Freiheiten betroffen ist. Zudem muss die Datenpanne an sich, ihre Auswirkungen sowie die ergriffenen Abhilfemaßnahmen umfangreich dokumentiert werden.

3.8 Sanktionen

Das BDSG sieht bisher nur einen Bußgeldrahmen von bis zu EUR 300.000,00 je Einzelfall vor. Bei einem Verstoß gegen Art. 5 DSGVO droht dann jedoch ein Bußgeld von bis zu EUR 20 Mio. oder – sofern höher – 4 % des weltweiten Jahresumsatzes. Dabei reicht es aus, dass dem Verantwortlichen der Nachweis der Einhaltung nicht gelingt, um von einem Verstoß auszugehen.[23]

Auch kleine Unternehmen müssen bei Verstößen mit Geldbußen in empfindlicher Höhe rechnen, denn sie sollen „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein". Die Aufsichtsbehörden machen keine konkreten Angaben dazu, wie hoch die Bußgelder ausfallen könnten.

Zusätzlich muss beachtet werden, dass Personen, die wegen eines Datenschutzverstoßes einen Schaden erlitten haben, Anspruch auf Schmerzensgeld haben, das, je nach Fall, bis zu mehreren tausend Euro betragen kann.

22 Lepperhoff & Müthlein (2017), Ziffer 12.2.3 b)

23 Lepperhoff & Müthlein (2017), Ziffer 7.1

3.9 Übersicht der Änderungen und Herausforderungen für KMU

Die folgende Übersicht fasst die vorangegangenen Beschreibungen der sich durch die Wirksamkeit der DSGVO ergebenden wichtigsten Änderungen zusammen und zählt auf, welche Herausforderungen sich für KMU in den jeweiligen Bereichen ergeben.

Thema	HERAUSFORDERUNGEN	Verweise
Anwendungsbereich	• Identifizieren der personenbezogenen Daten und datenschutzrelevanten Verarbeitungsprozesse, die von der DSGVO betroffen sind	Art. 2
Betroffenenrechte	• Entwicklung geeigneter Maßnahmen, die die Betroffenenrechte unverzüglich (spätestens innerhalb eines Monats) erfüllen	Art. 12 - 20
Dokumentation	• Identifizieren und zusammenfassen der bestehenden Lösungen für einzelne Prozesse • Geforderte Verfahrensverzeichnisse sind sehr umfangreich und umfassen neue Aufgaben	Art. 5 Art. 30
Auftragsdatenverarbeitung	• Identifizieren aller Auftragsdatenverarbeiter • Anpassen aller bestehenden Verträge	Art. 28 Art. 82
Datenschutz-Folgenabschätzung	• Korrekte Durchführung der Risikoanalyse • Reduzieren eines hohen Risikos durch angemessene technische und / oder organisatorische Maßnahmen	Art. 35
Technische und organisatorische Maßnahmen	• Stand der Technik ist ein unbestimmter Rechtsbegriff • IT-Sicherheit ist ein umfangreiches Thema • Es ist eine Vielzahl an vorbeugenden Maßnahmen zu beachten, z. B. in Bezug auf Berechtigungen, Verschlüsselungen, Kommunikation, Speicherung	Art. 25 Art. 32
Meldepflicht	• Etablierung von in der Praxis schnell funktionierenden Prozessen bei Datenpannen • Prognose über die Folgen einer Schutzverletzung ist schwer einzuschätzen	Art. 33 und 34
Sanktionen	• Das Einhalten aller Nachweispflichten ist notwendig, um keinen Verstoß zu begehen • Die Höhe der Bußgelder ist nicht absehbar, da es keine offiziellen Angaben (z. B. Bußgeldtabellen) gibt • Bei Verstößen muss mit finanziellem Schaden sowie mit Rufschädigung umgegangen werden	Art. 83 und 84

Tabelle 5: Übersicht der Änderungen und Herausforderungen für KMU
Quelle: eigene Zusammenstellung atene KOM GmbH

4 ADDITIVE MANUFACTURING

4.1 Begriffe, Verfahren und Anwendung

4.1.1 Begriffserklärungen

Im Gegensatz zu den klassischen subtraktiven Fertigungsverfahren wie Fräsen, Bohren und Drehen, bei denen Material abgetragen wird, um etwas herzustellen, wird bei der additiven Herstellung Material schichtweise hinzugefügt. Auf der Grundlage von digitalen Daten können so dreidimensionale Objekte aus verschiedenen Materialien wie Kunststoffen und Metallen unmittelbar gefertigt werden.

Additive Fertigung, Additive Manufacturing bzw. Generative Fertigungsverfahren werden unter dem Standard ISO/ASTM 52900:2015[24] wie folgt definiert:

> *„Additive manufacturing is the general term for those technologies that based on a geometrical representation creates physical objects by successive addition of material. These technologies are presently used for various applications in engineering industry as well as other areas of society, such as medicine, education, architecture, cartography, toys and entertainment."*

In der deutschen Übersetzung:

> *„Additive Fertigung ist der Oberbegriff für jene Technologien, die auf Basis einer geometrischen Darstellung durch sukzessives Hinzufügen von Material physikalische Objekte erzeugen. Diese Technologien werden gegenwärtig für verschiedene Anwendungen in der Maschinenbauindustrie sowie in anderen Bereichen der Gesellschaft wie Medizin, Bildung, Architektur, Kartographie, Spielzeug und Unterhaltung verwendet."*

Der Standard ISO/ASTM 52900:2015 wurde gemeinsam von den Standardisierungsorganisationen ISO und ASTM International im Dezember 2015 vorgestellt und führt die vorherigen Normen beider Organisationen zusammen. In diesem Standard werden die generellen Prinzipien und die Terminologie definiert.

In der Öffentlichkeit sind additive Fertigungsverfahren auch unter „Rapid Prototyping" und „3-D-Druck" bekannt. Diese Bezeichnungen sind nicht ganz korrekt, da es sich nicht um Oberbegriffe handelt, sondern bei Rapid Prototyping um ein Anwendungsfeld, in dem die Verfahren der additiven Fertigung zur Herstellung von Modellen und Prototypen genutzt werden und bei 3D-Druck um ein spezielles Verfahren innerhalb der additiven Fertigung.

24 ISO/ASTM. (2015, Dezember). ISO/ASTM 52900:2015. Abgerufen am 2. März, 2018 von https://www.iso.org/standard/69669.html

4.1.2 Additive Herstellungsverfahren

Es gibt eine Reihe verschiedener additiver Herstellungsverfahren. Die aktuell existierenden Anlagen und Technologien sind Gegenstand einer schnell voranschreitenden Forschung getrieben durch einen dynamischen, schnell wachsenden Markt. Manche Verfahren sind zudem im Prinzip sehr ähnlich und unterscheiden sich nur durch einige wenige Abänderungen, was eine Klassifikation der Verfahren erschwert. Faktoren, die bei den Herstellungsprinzipien eine Rolle spielen und zur Klassifikation herangezogen werden können sind vor allem der Ausgangszustand der zu verarbeitenden Stoffe (flüssig, plastisch, fest), das verarbeitete Material oder die Art, mit der das Material verbunden wird. Abhängig vom gewählten Material und Verfahren erzielen die gefertigten Produkte unterschiedliche Werte hinsichtlich Oberfläche, Farbwahl, Detailgenauigkeit oder Festigkeit.

Im Folgenden werden die wichtigsten Herstellungsverfahren, geordnet nach dem Ausgangszustand der zu verarbeitenden Stoffe, kurz aufgeführt.[25]

Bei den **pulverbasierten Prozessen** (festes Ausgangsmaterial) werden dünne Schichten eines Pulvers aufgetragen und verbunden. Dabei können Pulver aus verschiedenen Materialien wie Metall oder Keramik bestehen. **Selektives Lasersintern / Lasermelting (SLS)** ist ein Verfahren, das mit pulverförmigen Ausgangsstoffen arbeitet, die mit einem Laser in die gewünschte Form geschmolzen werden. Durch schicht- bzw. zeilenweises Aufschmelzen der entsprechenden Bereiche und anschließendes Abkühlen und Verfestigen einer dünnen gleichmäßigen Pulverschicht entstehen schichtweise komplexe Formen. Auch das Verfahren, das unter den Begriffen **3D-Druck oder Binder Jetting (BJ)** bekannt ist, ist ein pulverbasiertes Verfahren und beruht auf dem Verkleben von Partikeln miteinander. Diese werden allerdings nicht wie beim Selektiven Lasersintern mit einem Laser aufgeschmolzen, sondern unter Einsatz eines Bindemittels örtlich verklebt. Dieses Verfahren ermöglicht das Einfärben der gedruckten Teile.

Eine der populärsten Methoden ist die Herstellung mit geschmolzenen (plastischen) Ausgangsmaterialien. Hier wird das **Extrusionsprinzip** angewendet, welches das kontinuierliche Herauspressen von festen bis dickflüssigen härtbaren Massen unter Druck aus einer formgebenden

25 Zur Vertiefung siehe: Hessen Trade & Invest GmbH. (2015). Additive Fertigung. Der Weg zur individuellen Produktion. Abgerufen von http://www.haute-innovation.com/cms/upload/PDF/Additive_Fertigung_final_screen.pdf

Düse beschreibt. Anschließend wird das Material an einer gewünschten Stelle abgelegt. **Das Schmelzschichtverfahren / Fused Filament Fabrication (FFF)** oder **Fused Layer Modeling (FLM)** funktioniert nach diesem Prinzip und ist mit einer beweglichen Heißklebepistole vergleichbar. Kunststoffe haben einen hohen Stellenwert aber auch andere zähflüssige Materialien wie Lebensmittel, Beton oder Gips können verwendet werden. Dieses Verfahren zählt derzeit zu den günstigsten Lösungen.

Beim **Photopolymerisationsverfahren** werden flüssige Photopolymere (Kunststoff) durch UV-Strahlung miteinander vernetzt. Die **Stereolithografie (SLA)** ist das älteste additive Verfahren. Es wurde bereits in den 1980er Jahren entwickelt. Mithilfe eines Laserstrahls wird dabei eine einzelne Schicht des knapp unter der Oberfläche der flüssigen Photopolymere liegenden Werkstücks ausgehärtet. Das Werkstück wird anschließend um die Höhe einer neuen Schicht abgesenkt. Schrittweise entsteht dadurch ein dreidimensionales Modell.

Ein weiteres Verfahren der additiven Fertigung ist das **Schichtlaminatverfahren / Layer Laminate Manufacturing (LLM)**, das jedoch vergleichsweise wenig genutzt wird. Bei diesem Verfahren werden Schichten von Papier oder Folien übereinander verklebt und mittels Cutter automatisiert in die gewünschte Form gebracht. Für das Arbeiten mit Papier ist ebenfalls Paper Lamination Technology (PLT) eine gängige Bezeichnung.

4.1.3 Anwendungsfelder und -branchen

Im Entwurfsprozess eines neuen Produkts werden häufig Details verändert oder neue Konzepte umgesetzt. Eine Fertigung in Serienqualität ist oftmals zu teuer und zeitintensiv. Rapid Prototyping umfasst die additive Fertigung von Präsentationsmodellen und funktionellen Prototypen, deren Eigenschaften nahe am möglichen Serienmodell liegen. Diese Prototypen können schnell getestet und ausgewertet werden, auch wenn ein Ersatzmaterial verwendet wird.

Neben dem Rapid Prototyping gibt es das Anwendungsfeld Rapid Tooling für den Werkzeug- und Formenbau sowie Rapid Manufacturing für die flexible, schnelle Fertigung von Bauteilen und Serien. Gefertigte Produkte bestehen oft aus mehreren Komponenten, die in einer Mischung aus herkömmlichen und additiven Herstellungsverfahren angefertigt werden können.

Der Einsatz additiver Technologien kann aus einer Reihe von Gründen vorteilhaft sein:

- Komplexität der Bauteile: Das schichtweise Auftragen von Material erlaubt hochkomplexe Formen. Ein oft genanntes Beispiel sind natürliche bionische Strukturen. Funktionen können außerdem bereits während der Fertigung direkt in das Bauteil integriert werden.

- Interne Hohlstrukturen: Die additive Fertigung eignet sich sehr gut zum Erzeugen von internen Hohlstrukturen. Dadurch können beispielsweise unter der Oberfläche liegende Heiz- oder Kühlkanäle integriert werden.

- Ressourceneffizienz: Das Material wird genau an den Stellen aufgetragen, wo es benötigt wird. Beim klassischen Zerspanen ist der Ressourcenaufwand größer, da das Bauteil durch das Abtragen eines großen Materialblocks geformt wird.

- Reduzierung des Gewichts und der Teilezahl: Komplexe Bauteile können in einem Stück oder mit geringerer Teilezahl hergestellt werden, was den Aufwand für Konstruktion und Montage verringert. Durch integrierte Hohlräume können sowohl Ressourcen als auch Gewicht gespart werden.

- Schnelle und werkzeuglose Fertigung: Die additive Fertigung läuft nahezu werkzeuglos. Ein Anpassen von Gussformen oder anderen Produktionswerkzeugen entfällt.

- Logistischer Aufwand: Mit der Verbreitung additiver Fertigung können Ersatzteile und neue Produkte zunehmend dort produziert werden, wo sie benötigt werden. Lediglich die benötigten Daten müssen vorliegen. Ersatzteile stehen beispielsweise nach dem Datendownload und der lokalen additiven Fertigung direkt bereit.

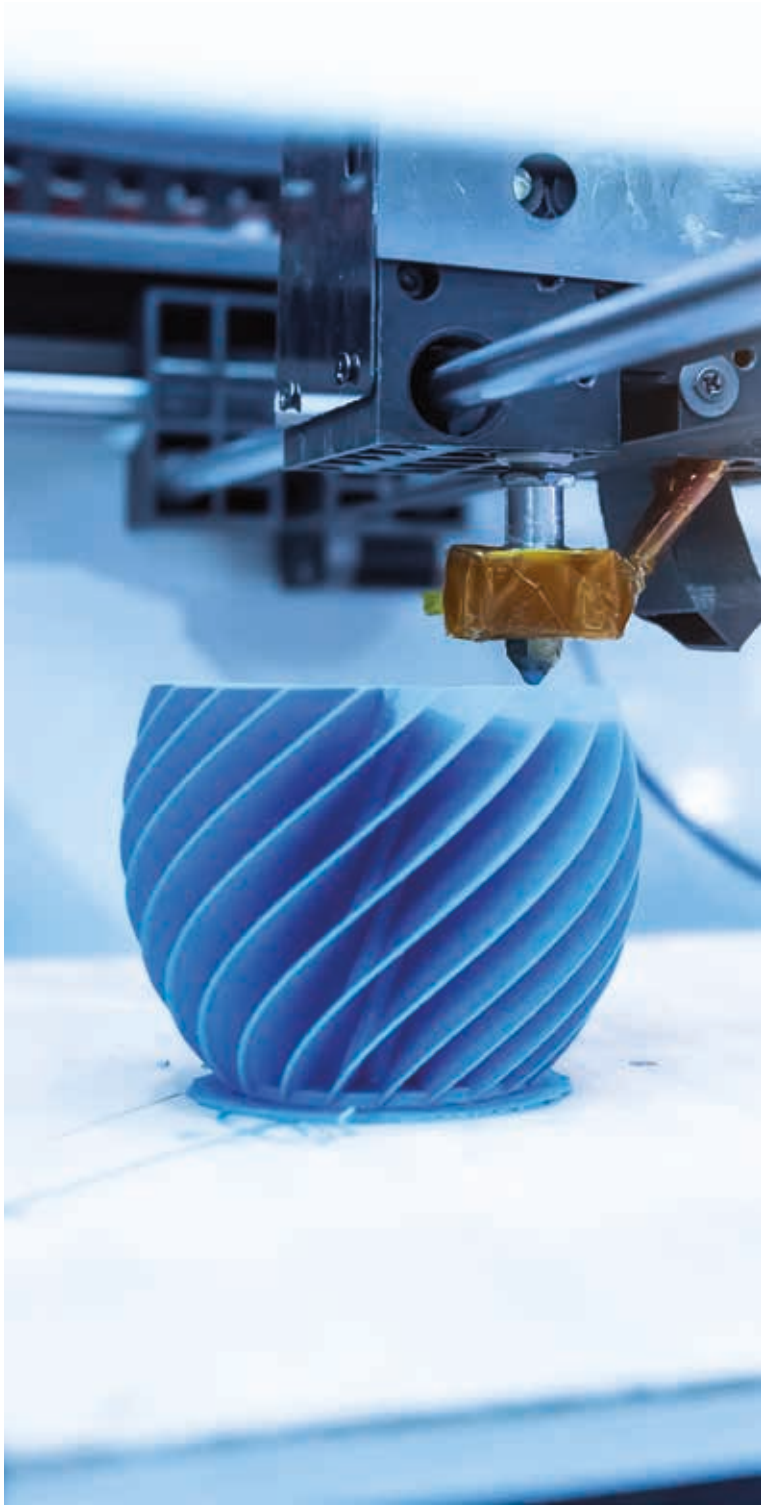
- Verkürzter Entwicklungsprozess: Durch die schnelle Verfügbarkeit von Prototypen und die Reduktion der Fertigungsschritte kommen neue Produkte schneller auf den Markt. Unternehmen können sich dadurch besser an geänderte Marktanforderungen anpassen.

- Individualisierbarkeit: Immer dort, wo Technik an den Menschen angepasst wird, entstehen durch die additive Fertigung neue Möglichkeiten zur individuellen Fertigung. Besonders in der Medizintechnik aber auch bei der Fertigung von Konsumgütern wie Sportgeräten oder Brillen können individualisierte Einzelstücke entstehen.

Beschränkt wird der Einsatz derzeit vor allem noch durch die begrenzte maximale Bauteilgröße und die eingeschränkte Eignung für Hochleistungslegierungen.

Die additive Fertigung hat sich in verschiedenen industriellen Branchen etabliert. Eine Vorreiterstellung in der Produktion nehmen die Medizintechnik und der Werkzeugbau ein. Aber auch stark durch die Serienproduktion geprägte Branchen wie die Automobilindustrie oder die Luft- und Raumfahrt setzen zunehmend auf additiv erzeugte Bauteile.

Additive Fertigung kommt regelmäßig in den folgenden Branchen zum Einsatz:



Branche	Bedeutung von Additiver Fertigung	Beispielprodukte
Medizintechnik	• Die Individualität eines jeden Menschen erfordert präzise passende Medizinprodukte • Einsatz ist bereit weit entwickelt – manche Produkte werden bereits fast ausschließlich additiv gefertigt	• Hörgeräte • Prothesen • Implantate (Zahnersatz) • Gewebe und Organe (Bioprinting)
Maschinen- und Werkzeugbau	• Hochkomplexe Formen werden möglich gemacht • Betrifft viele verschiedene Branchen, da die Herstellung von aufwendigen Werkzeugen fast immer die Grundlage für den Fertigungsprozess darstellt	• Bauteile für Maschinen • Greifsysteme (Robotik) • Kühlsysteme • Formeinsätze • Werkzeugreparatur
Luft- und Raumfahrtindustrie	• Stückzahlen sind oft so gering, dass additive Fertigung effizienter ist, als ein spezielles Werkzeug für die Serienproduktion zu bauen • Gewichtseinsparung ist ein besonders wichtiger Aspekt	• Triebwerkteile und Treibstoffrohre • Satellitenbauteile • unbemannte Luftfahrzeuge (UVA) • Interieur
Automobilindustrie	• Besonders relevant in der Entwicklung und bei Prototypen • Bei hochwertigen Sportwagen und im Rennsport, um Gewicht einzusparen • Bei Großserien typischerweise noch nicht im Einsatz	• Einspritzdüsen • Ersatzteile aus Kunststoff • Sitze • Schaltknöpfe
Elektrotechnik	• Großes Potenzial, denn Design- und Testzyklen können sich von Wochen auf wenige Tage reduzieren • Erst seit kurzem in diesem Bereich im Einsatz und noch in der Entwicklung	• Leiterplatten (PCB) • elektronische Schaltkreise • Antennen • Heizmuster • Sensoren
Lifestyleindustrie	• Ermöglicht das Herstellen von stabilen und leichten Produkten, sowie ungewöhnlichen Formen und Strukturen • Bisher hauptsächlich bei Produktentwicklung und -design; Individualisiertes Design direkt durch den Kunden noch selten	• Schmuck • Uhren • Brillengestelle • Bekleidung und Schuhe • Sportausrüstung • Spielzeug • Kameras und Zubehör
Architektur, Interieur, Design und Kunst	• Eröffnet neue Dimensionen der kreativen Gestaltung • Macht die Herstellung von belastbaren und gleichzeig leichten Baumaterialien möglich • Vor allem für Designer- und innovative Einzelstücke verwendet, weit entfernt von der Serienproduktion	• Neue Baumaterialien • Verbindungsteile • Modelle • Sitzmöbel • Lampen • Polsterfedern • Skulpturen
Nahrungsmittelindustrie	• Ermöglichen individuelle Nahrungsmittel als Kunstobjekte, persönliche Geschenke oder mit genauen Nährstoffinhalten • Lebensmitteldrucker befinden sich noch in der Entwicklung, es gibt viele Forschungs- und Testprojekte	• Schokolade • Zuckerformen • Pizza • Pasta • Pfannkuchen • Torten • Eiscreme

Tabelle 6: Branchen mit Einsatz von additiver Fertigung
Quelle: eigene Zusammenstellung atene KOM GmbH

Durch die Weiterentwicklung und den zunehmenden Preisverfall werden additive Technologien auch für private Anwender zunehmend interessant. Im sogenannten Maker Movement, einer Community von begeisterten Bastlern und Tüftlern, nehmen 3D-Drucker eine zentrale Rolle ein. Verschiedene Anwender vernetzen sich hier und tauschen Daten für den 3D-Druck.

4.2 Der Markt der additiven Fertigung in Deutschland und Hessen

4.2.1 Marktüberblick

Die Branche rund um die additive Fertigung umfasst neben den additiven Fertigungsanlagen auch Material, Zubehör, Software und Dienstleistungen, die mit der additiven Fertigung zusammenhängen. Das globale Wachstum dieses Marktes ist rasant: Für den Zeitraum 2004 bis 2014 zeigte der Markt eine jährliche Wachstumsrate von ca. 20 %, zwischen 2010 und 2014 lag das Wachstum sogar größer als 30 %. Bis 2020 wird dieses Wachstum weiterhin deutlich steigen – Wachstumsraten von bis zu 40 % pro Jahr werden erwartet.[26]

Für Güter, die mit der additiven Fertigung zusammenhängen, hat sich das weltweite Marktvolumen zwischen 2003 und 2013 versechsfacht.[27] Eine verlässliche aktuelle Schätzung des Marktvolumens additiv gefertigter Produkte liegt, laut der von der Bundesregierung eingerichteten Expertenkommission Forschung und Innovation, jedoch nicht vor. 2016 lag es laut „Wohlers Report 2017" bei 6,1 Milliarden US-Dollar.[28] Auch die Zahl der Patente und Publikationen ist in den letzten Jahren stark gestiegen. Verschiedene Studien liefern Prognosen, die für 2020 ein Volumen zwischen 7 und 21 Mrd. US Dollar voraussagen.

Die Ausgabe 2017 des jährlichen Reports „The state of 3D printing" des Unternehmens sculpteo, basiert auf einer Befragung von 1.000 Unternehmen weltweit, die additive Fertigungsverfahren verwenden.[29] Die Branchensegmentierung der Befragten wird angeführt von Konsumgütern und Industriegütern mit jeweils 17 %, gefolgt von 13 % High-Tech-Bereich, 9 % Dienstleistungssektor und 7 % aus dem Gesundheitswesen. Die stärksten Einzelbranchen sind Elektronik mit 7 %, mechanische und metallverarbeitende Industrie und Automobilindustrie mit jeweils 5 % sowie Luft- und Raumfahrt mit 4 %. Noch einmal 6 % macht der Bildungssektor aus.

90 % der Unternehmen, die additive Herstellungsmethoden nutzen, sehen darin einen Wettbewerbsvorteil. 72 % gehen davon aus, dass ihre Ausgaben für die additive Fertigung im Jahr 2018 steigen werden.

Additive Fertigungsverfahren werden aktuell hauptsächlich zum Prototyping (34 %) und zum Proof of Concept (Machbarkeitsnachweis) (23 %) angewendet. Additive Fertigung wird dadurch zu 57 % in der Entwicklungsphase von neuen Produkten angewendet. Danach folgt die Anwendung in der finalen Herstellung von Produkten (22 %) und in der Herstellung von Marketingbeispielen (10 %).

Das am häufigsten verwendete Material ist Kunststoff (88 % der Befragten). Harze werden von 35 % und Metall von 28 % der Befragten verwendet. Bezüglich der Herstellungsverfahren ist das Schmelzschichtverfahren (FDM) die meistgenutzte Technologie (36 %), gefolgt von Selektivem Lasersintern (SLS, 33 %) und Stereolithographie (SLA, 25 %).

26 Roland Berger. (2016). Additive Manufacturing - next generation AMnx. Abgerufen von https://www.rolandberger.com/de/press/Neue-Studie-Rasanter-Fortschritt-bei-3D-Druck-Systemen.html

27 Expertenkommission Forschung und Innovation. (2015). Additive Fertigung („3D-Druck"). Abgerufen von https://www.e-fi.de/fileadmin/Inhaltskapitel_2015/2015_B4.pdf

28 Krämer, A. (2017, 10. April). Wohlers Report 2017 verzeichnet 17,4 Prozent Wachstum in der weltweiten 3D-Druck-Industrie. Abgerufen 6. März, 2018, von https://www.3d-grenzenlos.de/magazin/marktforschung/wohlers-report-2017-3d-druck-27253733/

29 sculpteo. (2017). The state of 3D printing. Abgerufen von https://www.sculpteo.com/media/ebook/State%20of%203DP%202017_1.pdf

4.2.2 Additive Fertigung in Deutschland

In Deutschland und anderen technologisch führenden Ländern verbreiten sich die additiven Fertigungsverfahren schnell. Trotzdem wird laut aktuellem Bericht des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung des deutschen Bundestags[30] auch in den nächsten zehn Jahren noch keine flächendeckende Verbreitung erwartet.

Im internationalen Vergleich steht Deutschland auf der Liste angemeldeter Patente auf dem vierten Platz nach den USA, Japan und China.[31] Deutschland ist vor allem bei der Entwicklung von Verfahren, Materialien und Fertigungsanlagen vertreten. Insbesondere bei Verfahren zur Metallverarbeitung (Lasersintern) hat Deutschland mit einigen weltmarktführenden Unternehmen eine Vorreiterrolle, während der Bereich der Kunststoffverarbeitung von den USA dominiert wird. Zunehmende Bedeutung gewinnen Dienstleistungsunternehmen im Bereich Rapid Prototyping, die für die deutsche Industrie tätig sind und Prototypen sowie Kleinserien entwickeln und fertigen.

Zwar haben sich die Verkaufszahlen von industriellen Anlagen zur additiven Fertigung zwischen 2010 und 2014 mehr als verdreifacht, dennoch liegt Deutschland in Bezug auf die industrielle Anwendung im internationalen Vergleich zurück. Die Bundesregierung sieht hier die zentrale Herausforderung für die nächsten Jahre. Aktuelle Zahlen zum Marktvolumen in Deutschland liegen nicht vor. Schätzungen gingen für das Jahr 2016 von etwa 1 Mrd. Euro aus. Dies entspricht 10 % des globalen Umsatzes.[32] Im Jahr 2010 lag der Anteil bei ca. 15 bis 20 %. Bei einer breiten Definition von AF-Gütern, die neben dem Druck auch die Datenaufnahme und -aufbereitung beinhaltet, waren 2010 in Deutschland etwa 1.000 Unternehmen im Bereich additiver Fertigung tätig.[33]

Die Struktur von Unternehmen in der additiven Fertigung entspricht der üblichen Unternehmensstruktur in Deutschland: Knapp die Hälfte beschäftigt weniger als 25 Mitarbeiter und erwirtschaftet einen jährlichen Umsatz von unter 5 Mio. Euro. Im Hinblick auf die EU-Kriterien sind etwa 90 % der Unternehmen dem Mittelstand zuzuordnen.

Mit dem Umsatz und der Anzahl der Unternehmen wächst auch der Arbeitsmarkt. Laut der Plattform Joblift stieg die Anzahl der ausgeschriebenen Stellen 2017 im Vergleich zum Vorjahr um 88 %. Hauptsächlich kleine Unternehmen hatten diese Stellen ausgeschrieben.

Die Bundesregierung fördert die additive Fertigung hauptsächlich im Bereich Forschung und Entwicklung. Hier wurden im Rahmen der Projektförderung zwischen 2003 und 2013 über 21 Mio. Euro vergeben. Eine übergeordnete politische Förderstrategie für die additive Fertigung gibt es jedoch bisher nicht. Das Thema ist u. a. im Rahmen der aktuellen High-Tech Strategie von 2014 angesiedelt. In den letzten Jahren wurden verschiedene Förderrichtlinien z. B. „Additive Fertigung – Individualisierte Produkte, komplexe Massenprodukte, innovative Materialien“[34] sowie „Materialwissenschaft und Werkstofftechnologien – Themenschwerpunkt: Materialien für die Additive Fertigung“[35] veröffentlicht. Zudem gibt es das themenoffene Regionalförderprogramm Zwanzig20, in dessen Rahmen das BMBF additive Fertigung fördert. Hier stehen von 2013 bis 2020 bis zu 45 Mio. Euro zur Verfügung.[36]

30 Deutscher Bundestag. (2017). Technikfolgenabschätzung (TA) Additive Fertigungsverfahren „3-D-Druck“ (Bericht des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung (18. Ausschuss) gemäß § 56a der Geschäftsordnung). Abgerufen von http://dip21.bundestag.de/dip21/btd/18/134/1813455.pdf

31 Richter, S.; Wischmann, S. (2016). Additive Fertigungsmethoden – Entwicklungsstand, Marktperspektiven für den industriellen Einsatz und IKT-spezifische Herausforderungen bei Forschung und Entwicklung (Eine Studie im Rahmen der Begleitforschung des Technologieprogramms AUTONOMIK für Industrie 4.0 des Bundesministeriums für Wirtschaft und Energie). Abgerufen von https://vdivde-it.de/sites/default/files/document/Additive-Fertigungsmethoden-2016.pdf

32 Statista. Geschätzter Umsatz mit 3D-Druck-Produkten in Deutschland und weltweit im Jahr 2016 (in Milliarden Euro). Abgerufen 2. März, 2018, von https://de.statista.com/statistik/daten/studie/581411/umfrage/umsatz-mit-3d-druck-in-deutschland-und-weltweit/

33 Astor, M.; von Lukas, U.; Jarowinsky, M. et al. (2013). Marktperspektiven von 3D in industriellen Anwendungen. Abgerufen von https://www.prognos.com/uploads/tx_atwpubdb/130117_Prognos_IGD_MC_Studie_3D_Maerkte.pdf

34 Bundesministerium für Bildung und Forschung. (2015, 27. März). Bekanntmachung des Bundesministeriums für Bildung und Forschung von Richtlinien zur Förderung im Themenfeld „Additive Fertigung – Individualisierte Produkte, komplexe Massenprodukte, innovative Materialien (ProMat_3D)“. Abgerufen 2. März, 2018, von https://www.bmbf.de/foerderungen/bekanntmachung-1037.html

35 Bundesministerium für Bildung und Forschung. (2016, 15. März). Bekanntmachung Richtlinie zur Förderung transnationaler Forschungsprojekte innerhalb des ERA-NET „M-era.Net II“ „Materialwissenschaft und Werkstofftechnologien“ – Themenschwerpunkt: Materialien für die Additive Fertigung – in den Rahmenprogrammen „Vom Material zur Innovation“ und „Innovationen für die Produktion, Dienstleistung und Arbeit von morgen“. Abgerufen 2. März, 2018, von https://www.bmbf.de/foerderungen/bekanntmachung-1173.html

36 Expertenkommission Forschung und Innovation (2015), S. 75

4.2.3 Additive Fertigung in Hessen

Insgesamt sind im Süden Deutschlands mehr Unternehmen angesiedelt als im Norden. Im Jahr 2012 hatte fast die Hälfte der Unternehmen der additiven Fertigung ihren Sitz in Bayern und Baden-Württemberg. Weitere 17,7 % waren in Nordrhein-Westfalen gemeldet. Daneben hat nur noch Hessen mit einem Anteil von 8,3 % eine überdurchschnittlich hohe Dichte an Dienstleistern der Branche. Die übrigen Bundesländer liegen zwischen 5,5 % (Niedersachsen) und 0,6 % (Mecklenburg-Vorpommern) der deutschen Unternehmen.

In Hessen haben sich einige größere Unternehmen und Forschungseinrichtungen angesiedelt. Die additive Fertigung ist ein wichtiger Treiber der Entwicklungen für viele weitere Branchen. Aktuell (2018) sind etwa 30 – 40 Unternehmen und Forschungseinrichtungen aus diesem innovativen Arbeitsfeld in Hessen ansässig. Die regionale Verteilung ist für Hessen typisch – sie sind vor allem in Südhessen und teilweise auch in Mittelhessen zu finden, in Nordhessen dagegen kaum.

Es sind Unternehmen verschiedenster Branchen angesiedelt, die additiv fertigen oder entsprechende Produkte beziehen. Darunter fällt z. B. die Automobilbranche, in der additiv hergestellte Werkzeuge für die Fertigung genutzt werden oder die mögliche Herstellung von bionisch inspirierten Karosserien untersucht wird. Unter den Anbietern befindet sich ein auf Lasersintern spezialisiertes Unternehmen sowie Unternehmen für die Fertigung von Prototypen.

Zudem gibt es in Hessen wichtige Hochschulen und Institute, die sich der Forschung zu additiver Fertigung widmen. Ein wichtiges Zentrum ist Darmstadt, wo die Technische Universität im Bereich Medizintechnik und das Fraunhofer-Institut für Betriebsfestigkeit und Systemzuverlässigkeit LBF im Bereich Materialien forschen. Im FabLab der TU Darmstadt beim Fraunhofer Institut für Graphische Datenverarbeitung IGD können auch Privatpersonen kostenlos Technologien nutzen. Auch die Europäische Weltraumbehörde ESA hat hier einen Standort, das sogenannte European Space Operations Centre, wo Techniken zum Bau einer Mondstation getestet werden.

Die Philipps-Universität Marburg sowie die Universität Kassel führen Forschungsprojekte zur additiven Fertigung von Baumaterialien und Keramiken für die Dentalmedizin durch. Die Hochschule für Gestaltung Offenbach beschäftigt sich mit Industriedesign im Kontext der additiven Fertigung.[37]

Das Land Hessen hat sich die Digitalisierung in allen Wirtschafts- sowie Lebensbereichen zur zentralen Aufgabe gemacht und will die Chancen nutzen, die sich daraus ergeben für die Bewältigung gesellschaftlicher Herausforderung, für die positive Entwicklung der Wirtschaft und Arbeitsbedingungen und für die Stärkung der Innovationskraft Hessens. Vor diesem Hintergrund hat die Hessische Landesregierung die „Strategie Digitales Hessen, Intelligent. Vernetzt. Für Alle“[38] verfasst, welche die Förderung von Innovationsprojekten und den Aufbau von Kompetenzzentren im Bereich des 3D-Drucks vorsieht.

Auch im Rahmen der neuen Dachmarke „Technologieland Hessen“ ist die additive Fertigung ein wichtiges Feld, das im Thema „Produktion“ angesiedelt ist. Das Technologieland Hessen hat sich zum Ziel gesetzt, diese Fertigungstechnologie durch die vielseitige Unterstützung von Unternehmen und Forschungseinrichtungen voranzutreiben.

37 Zur Vertiefung der Unternehmen/Forschungseinrichtungen siehe: Hessen Trade & Invest GmbH. (2015)

38 Hessische Landesregierung. (2016). Strategie Digitales Hessen. Intelligent. Vernetzt. Für Alle. Abgerufen von https://www.digitalstrategie-hessen.de/img/Digitalstrategie_Hessen_2016_ver1.pdf

4.3 Datenverarbeitung im Produktionsprozess

4.3.1 Begriffliche Grundlagen

CAD steht für Computer Aided Design. Dies bedeutet computergestütztes Konstruieren, also der Entwurf von Produkten mit computerunterstützter Grafikerstellung. CAD läuft in den drei Phasen Konzipierung, Gestaltung und Detaillierung ab. Der Detailentwurf mit den zugehörigen Stücklisten und Fertigungsunterlagen kann anschließend von der computergestützten Arbeitsplanung (CAP) übernommen werden. 3D-CAD-Systeme können anhand einer Vielzahl von dafür vorgesehenen 3D-CAD-Programmen erzeugt werden.

Für die additive Fertigung ist eine Umwandlung in das **STL-Format** nötig – das aktuelle Standarddateiformat für den 3D-Druck. Das STL-Format beschreibt die Oberfläche von dreidimensionalen Objekten mit Hilfe von Dreiecken. Es wandelt die Modelloberfläche in eine Vielzahl von Dreiecken um. Für jedes Dreieck werden die Koordinaten der Eckpunkte und die Normale der Oberfläche gespeichert. Je kleiner diese Dreiecke sind, desto genauer kann eine gewünschte Form dargestellt werden. Dies ist insbesondere bei Krümmungen relevant, um Abweichungen vom Entwurf zu minimieren. Die meisten CAD-Programme können ein 3D-Modell als STL-Datei exportieren. STL transportiert nur die geometrischen Informationen des Modells und hat daher in der Regel eine verhältnismäßig geringe Größe. Ein weiterer Vorteil der Reduzierung der Modelle auf die Position der Dreiecke ist, dass nur Daten erhalten bleiben, die zur Produktion absolut nötig sind.

Die korrekte und sinnvolle Platzierung des Modells im Raum wird **Bauteilorientierung** genannt. Die Bauteilorientierung kann Einfluss auf das Ergebnis haben in Bezug auf die Genauigkeit, Oberflächenbeschaffenheit, mechanisch-technologischen Eigenschaften, Bauzeit, Kosten, Post Processing sowie auf die Stützkonstruktion insofern eine verwendet werden muss. Diese ist notwendig, um dem Modell beim Druck temporären Halt zu geben. Diese Struktur ist dabei aus dem gleichen Material wie das Modell selbst.

Unter Slicen versteht man das Zerlegen des Modells in einzelne horizontale Schichten, die dann an den Drucker weitergeleitet werden. Der Slicing-Prozess wird durch eine Slicer-Software durchgeführt und beinhaltet das Festlegen einiger Parameter wie z. B. Füllgrad, Layerhöhe und Geschwindigkeiten. Das Ergebnis ist der sogenannte **G-Code**. In ihm stehen auch Daten zum Heizbett und zum Druckkopf wie Temperatur und Geschwindigkeit sowie Informationen zum Vorschub des Filaments.

4.3.2 Prozesskette der additiven Fertigung

Trotz vieler unterschiedlicher Verfahren und Technologien, kann in der additiven Fertigung eine Reihe grundlegender Schritte identifiziert werden, die in jedem Fall durchlaufen werden müssen:

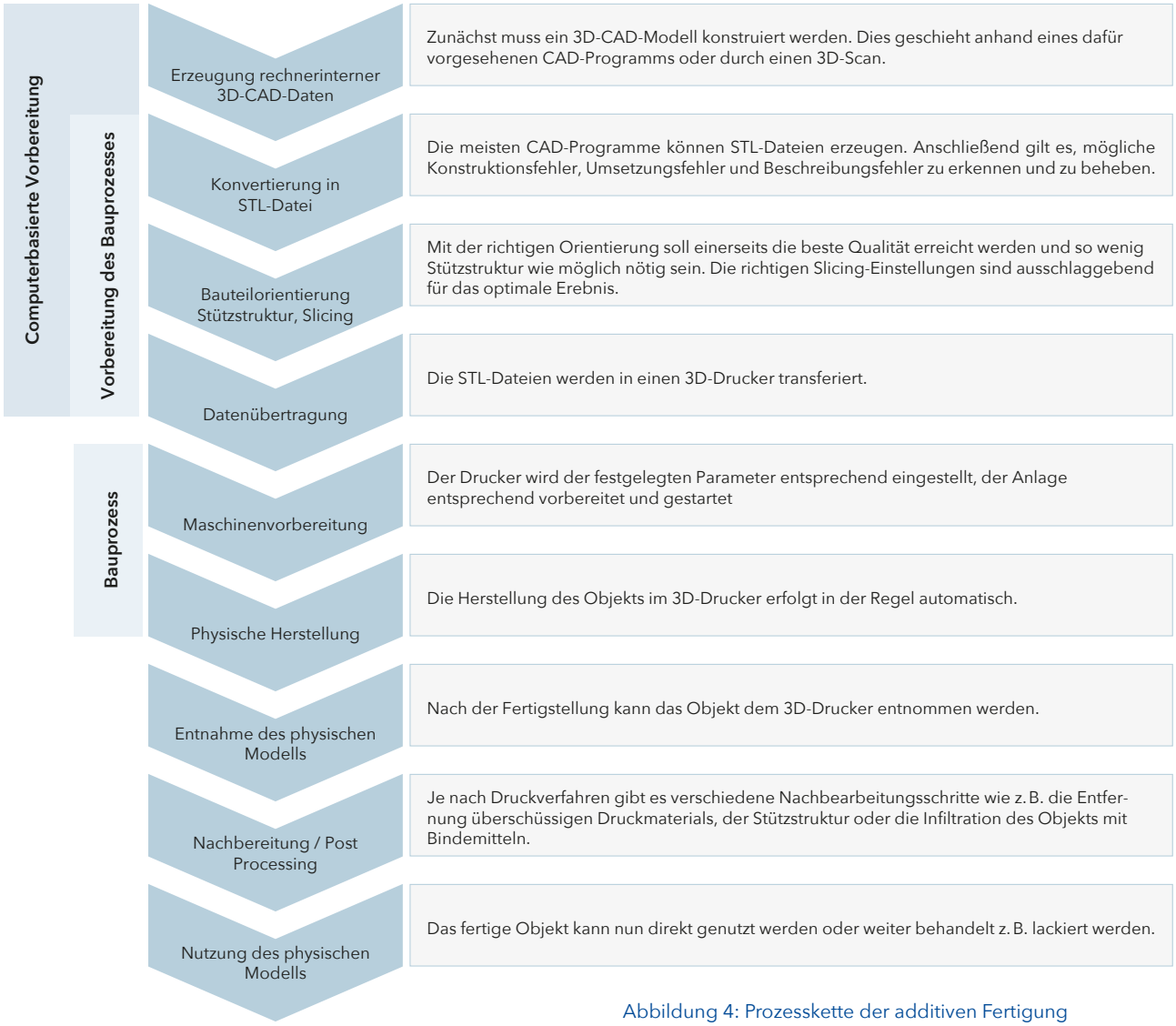


Abbildung 4: Prozesskette der additiven Fertigung
Quelle: Eigene Darstellung nach Anderl (2014)[39]

39 Anderl, R., & Arndt, A. (2014, 24. September). Additive Manufacturing oder generative Fertigungsverfahren – vom Prototypen zur Massenfertigung? Abgerufen 1. Februar, 2018, von https://www.hessen-nanotech.de/mm/mm001/3D_Additive_Manufacturing_Anderl_TUD.pdf

4.4 Personenbezogene Daten in der additiven Fertigung

4.4.1 Analyse nach Unternehmensbereichen

Der Annahme, dass Datenschutz in der Branche der additiven Fertigung eine wichtige Rolle spielt, liegen folgende Tatsachen zu Grunde:

- Die Additive Fertigung ermöglicht eine individualisierte Produktentwicklung, kleine Stückzahlen und sogar Einzelstücke, die je nach Bedürfnissen, Anforderungen und Wünschen des Kunden angefertigt werden können.
- Die additive Fertigung von Produkten basiert auf Daten, die der Maschine / Anlage Informationen darüber geben, welche Form das gewünschte Produkt haben soll. Viele individuelle Produkte bedeuten also auch viele verschiedene Datensätze.
- Die Unternehmen, die über additive Fertigungsanlagen verfügen, stellen in der Regel maßangefertigte Produkte für eine Vielzahl verschiedener Kunden her und nehmen ggf. externe Dienstleister für einzelne Arbeitsschritte in Anspruch.
- Wie andere Unternehmen auch, beschäftigen Unternehmen aus dem Bereich der additiven Fertigung selbst Mitarbeiter

Auf Grundlage dieser vier Aspekte soll nun betrachtet werden, inwiefern in den zugehörigen Unternehmensbereichen – Produktentwicklung, Produktion, Kunden- und Personalmanagement – jeweils personenbezogene Daten, also Daten, die einer bestimmten Person zugeordnet werden können, vorkommen und verarbeitet werden können.

Individuelle Produktentwicklung
Individuelle Produkte sind auf ein Individuum und seine speziellen Bedürfnisse zugeschnitten. Ob nun bei dem Auftrag zur Herstellung ein Bezug zu einer natürlichen Person vorliegt oder nicht, ist dementsprechend davon anhängig, ob es sich bei dem Auftraggeber um eine Person handelt oder nicht bzw. das Produkt für eine Person angefertigt wird oder nicht. Wird zum Beispiel ein Implantat für einen Patienten gefertigt und dem Auftrag liegen Name und Krankenversicherungsnummer bei, ist hier ein deutlicher Personenbezug vorhanden. Ebenso verhält es sich, wenn eine Person beispielsweise einen Sportschuh nach den Maßen der Füße additiv anfertigen lässt. Die personenbezogenen Daten, die hierfür Verwendung finden können sind z. B. physische Merkmale,Gesundheitsdaten und persönliche Vorlieben.

Individuelle Produkte sind aber nicht immer auf eine Person zugeschnitten. Ebenso kann ein Unternehmen ein bestimmtes Bauteil oder Werkzeug konzipieren, entwickeln und herstellen lassen – ein Produkt dem kein personenbezogenes Datum anhängt.

Datengetriebene Produktion
Betrachtet man den Produktionsprozess der additiven Fertigung isoliert, werden nur unter bestimmten Umständen personenbezogene Daten verarbeitet. Wie im Kapitel 4.3 beschrieben, basiert die Produktion auf CAD-Daten, die in STL-Dateien umgewandelt werden. Damit schrumpft die Datenmenge erheblich und beinhaltet lediglich die Koordinaten der Eckpunkte der Dreiecke, die die Form beschreiben. Diese Daten sind zunächst nicht personenbezogen. Anders als bei anderen Austauschformaten wie JPEG (EXIF) oder PDF gibt es in STL-Dateien keinen Hinweis etwa auf Fotograf und Kameramodell oder Autor und Speicherdatum des Dokuments. Ein Personenbezug wäre nur möglich, wenn der Dateiname nicht pseudonymisiert ist oder weitere verbundene Dokumente Rückschlüsse zulassen würden. Also gilt auch hier: wenn keine Verbindung zu einer natürlichen Person möglich ist, werden in der Produktion keine personenbezogenen Daten verarbeitet.

Das ist allerdings nur für STL-Dateien uneingeschränkt richtig. Weil der seit 30 Jahren genutzte Standard nur die Oberfläche von Objekten beschreibt, aber keine Angaben über Material, Farbe oder maschinenspezifische Anweisungen für den generativen Fertigungsprozess erlaubt, werden seit 2010 Austauschformate entwickelt, mit denen zum Beispiel 3D-Drucker direkt angesteuert werden können. Selbst STL vergleichbare Formate, die wie STEP oder IGES nur grafische Primitive transportieren, und komplexere Standards wie 3MF, AMF oder VRML definieren im Header Felder für Metadaten, die zumindest potenziell personenbezogene Daten enthalten können: Autor, Bearbeiter, Speicherdatum und vieles mehr. Je weiter sich die Steuerung der additiven Fertigung in eine solche „Druckdatei" selbst verlagern lässt, desto mehr Möglichkeiten der Automatisierung ergeben sich auch für neue Geschäftsmodelle: Kunden könnten über eine Plattform in einem unterbrechungsfreien Workflow ihre Entwürfe praktisch selbst produzieren, indem sie die generative Fertigungsumgebung des Dienstleisters als

verlängerte Werkbank benutzen, inklusive Materialanforderung beim ERP-System (Enterprise Resource Planning) und anderen Bausteinen integrierter Fertigung. Dies wäre im Ablauf für den Auftraggeber nicht komplizierter als der Ausdruck einer Textdatei auf dem Bürodrucker. Seine personenbezogenen Daten würden in einem solchen Prozess bis zum Ende der Fertigungskette mittransportiert.

Kundenmanagement
Unternehmen der additiven Fertigung verfügen über Kundendaten, die es zu schützen gilt. Da die technischen Anlagen (3D-Drucker, zugehörige Materialien und Software) relativ kostenintensiv sind und es eine Vielzahl von Technologien gibt, die unterschiedliche Möglichkeiten bieten (vgl. 4.1), nutzen kleine und große Unternehmen der additiven Fertigung im Bedarfsfall auch die Dienste anderer Unternehmen. Zudem arbeiten die meisten Unternehmen in irgendeiner Art und Weise mit externer Dienstleister (z. B. Lieferanten, IT, Logistik) zusammen.

Es ist davon auszugehen, dass Unternehmen der additiven Fertigung grundsätzlich personenbezogene Daten sammeln – von Privatkunden, den Mitarbeitern von Unternehmenskunden und Mitarbeitern externer Dienstleister. Dazu gehören z. B. Personalien, Adressdaten, Kontaktdaten und ggf. physische Merkmale und Besitzmerkmale. Eine Kundendatenbank oder ein CRM-System (Customer-Relationship-Management) sind die gängigen Instrument zur Speicherung und Verwendung dieser Daten.

Personalmanagement
Auch der Schutz personenbezogener Daten der eigenen Mitarbeiter ist rechtlich geregelt. Diese Daten sind – wie die Daten aus dem Kundenmanagement – kein Spezifikum der additiven Fertigung, sondern betreffen branchenübergreifend alle Unternehmen.

Zu den Mitarbeiterdaten gehören neben Personalien, Kennnummern (Sozialversicherung, Steuer, Krankenversicherung), Bankdaten und Gehalt u. a. auch Daten zu Bildung, Qualifikationen und Leistung des Einzelnen.

4.4.2 Analyse nach Branchen

Wie in Kapitel 4.1 beschrieben, wird die additive Fertigung in vielen verschiedenen Branchen verwendet. Diese unterscheiden sich nach Art der verarbeiteten personenbezogenen Daten und wie diese verarbeitet werden.

In der **Medizintechnik** gibt es viele Bereiche, in denen personenbezogene Daten – darunter auch sensible Daten – erfasst und verarbeitet werden, z. B. Gesundheitsdaten, biometrische Daten oder physische Merkmale. Dies ist insbesondere in der Prothetik und Dentaltechnik der Fall, wo an den Körper angepasste Objekte – z. B. Prothesen, Zahnersatz, Implantate – angefertigt werden. Das Unternehmen, welches diese Teile für den Patienten additiv herstellt, benötigt zur Ausführung eines Auftrags jedoch in der Regel lediglich die Fertigungsdaten ohne Zuordnung zum Patienten. Die Beauftragung verläuft in der Regel über die Ärzte, Kliniken oder Krankenkassen, welche die Daten ohne Personenbezug an die fertigenden Unternehmen übermitteln.

Die **Lifestyleindustrie** sowie **Architektur**, **Interieur**, **Design** und **Kunst** sind vermutlich die Branchen, in der Unternehmen der additiven Fertigung am häufigsten selbst mit personenbezogenen Daten umgehen. Insbesondere bei einem privaten Kundenauftrag werden zunächst allgemeine Personendaten sowie Kundendaten aufgenommen. Je nach anzufertigendem Objekt können zudem personenbezogene Daten zu physischen Merkmalen (z. B. bei Kleidung, Schuhen oder 3D-Miniaturfiguren), persönlichen Vorlieben / Hobbies (z. B. bei Sportgeräten, Kamerateilen), Besitzmerkmalen (z. B. Modelle von Häusern) oder sogar zum Familienstand (z. B. bei Eheringen) anhand der anzufertigenden Objekte gesammelt werden.

Auch in der **Nahrungsmittelindustrie** ist die Verarbeitung von personenbezogenen Daten durch die fertigenden Unternehmen möglich, denkt man zum Beispiel an persönlich gestaltete und beschriftete Schokoladenobjekte oder an Diätnahrung, die eine bestimmte Person aufgrund einer körperlichen Kondition oder Krankheit zu sich nehmen muss – in diesem Fall läge sogar ein sensibles Datum vor.

Die Relevanz personenbezogener Daten in diesen Branchen wird sicherlich mit voranschreitender Entwicklung der Technik, Reduzierung der Kosten und Einführung der additiven Fertigung in weiteren Lebensbereichen in Zukunft an Bedeutung zunehmen.

In der **Automobilindustrie** ist die Relevanz spezifischer personenbezogener Daten geringer, insbesondere da in dieser Branche die meisten Unternehmen große industrielle Kunden bedienen und neben eigenen und

Kunden-Mitarbeiterdaten, zumeist kein Bezug zwischen einer natürlichen Person und den Daten rund um das zu fertigende Produkt besteht. Ausnahmen könnten sich ggf. ergeben, wenn z. B. Automobilersatzteile oder maßangefertigte Innenausstattung direkt vom Autobesitzer und nicht durch den Hersteller bestellt werden.

In den Branchen **Maschinen- und Werkzeugbau**, in denen additive Fertigung bereits eine große Rolle spielt, gibt es – auch nach eigener Aussage von Branchenvertretern – so gut wie keine personenbezogenen Daten, die spezifisch im additiven Fertigungsprozess auftauchen. In der **Luft- und Raumfahrtindustrie** sowie in der **Elektrotechnik** verhält es sich ähnlich.

4.4.3 Analyse nach Geschäftsbeziehungen

In den vorherigen Betrachtungen nach Unternehmensbereich und Branche wurde bereits mehrfach angesprochen, dass die Wahrscheinlichkeit bzw. die Relevanz der Verarbeitung personenbezogener Daten davon abhängig sind, ob der Auftraggeber ein Unternehmen oder der Endkunde ist. Die Verarbeitung personenbezogener Daten in Unternehmen wird daher abschließend im Hinblick auf die Geschäftsbeziehungen bzw. Art der Kunden betrachtet.

Business-to-Business (B2B)
Business-to-Business (B2B) bezeichnet Geschäftsbeziehungen zwischen mindestens zwei Unternehmen. Ein Großteil der Unternehmen aus dem Bereich der additiven Fertigung betreibt B2B, da sie Teile für die verschiedensten Industriebranchen anfertigen, insbesondere im Anwendungsfeld des Rapid Prototyping. Hinsichtlich Datenschutz stehen für diese Unternehmen Mitarbeiterdaten im Vordergrund – der eigenen und der von Kundenunternehmen und Dienstleistern. Andere personenbezogene Daten stellen eher eine Ausnahme dar.

Business-to-Consumer (B2C)
Es gibt auch zunehmend Unternehmen, die Geschäftsbeziehungen mit Privatpersonen (Konsumenten, Kunden) – auch Business-to-Consumer oder B2C genannt – pflegen und 3D-Druck für private Nutzer anbieten. Unternehmen in diesem Bereich bieten oftmals individualisierten 3D-Druck für alle erdenklichen Gegenstände an; von Ersatzteilen für Elektrogeräte über Bauteile für die eigene Hobbywerkstatt bis hin zu künstlerischen Skulpturen und Designermöbeln für die Innenausstattung. Andere Unternehmen haben sich auf die Herstellung von Produkten wie z. B. Schokolade[40], Brillen[41], 3D-Figuren von Personen[42] oder Spielzeug[43] spezialisiert. Dass im B2C-Bereich weit mehr personenbezogene Daten gesammelt und verarbeitet werden als im B2B-Bereich, liegt auf der Hand. Dementsprechend sind auch die Anforderungen an diese Unternehmen im Hinblick auf den Datenschutz umfangreicher.

Da der B2C-Bereich im Vergleich zum B2B-Bereich aktuell noch eine geringere Rolle spielt, sind vergleichsweise wenige Unternehmen betroffen. Mit voranschreitender Technik ergeben sich jedoch immer mehr Möglichkeiten und die Branche wächst: Viele Start-ups nutzen diese neuen Möglichkeiten als Chance, um mit innovativem Service und individuell gestalteten Produkten erfolgreich in den Markt einzutreten. Zwar sind die initialen Investitionskosten für 3D-Drucker und andere additive Fertigungsanlagen noch hoch, das Absinken des Preisniveaus ist aber absehbar – eine Entwicklung, die besonders kleine Unternehmen und Start-ups begünstigt.

4.4.4 Fazit

Die Relevanz personenbezogener Daten in der additiven Fertigung nach Unternehmensbereichen, Branchen und Art der Geschäftsbeziehungen (Kunden) ist in Tabelle 7 dargestellt.

Insgesamt ist festzustellen, dass sich die Art und die Menge personenbezogener Daten, die in der additiven Fertigung verarbeitet werden, von Unternehmen zu Unternehmen unterscheiden und von verschiedenen Faktoren abhängen.

Jedes Unternehmen muss dementsprechend seine individuellen Prozesse analysieren, um zu identifizieren, in welchen Unternehmensbereichen personenbezogene Daten verarbeitet werden, wo Risiken bei der Verarbeitung personenbezogener Daten auftauchen könnten und welche Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit besonders relevant sind.

40 http://www.schokoladendruckerei.de/
41 https://www.framepunk.com/
42 https://www.figurenwerk.de/
43 http://www.tinkertoys.de/

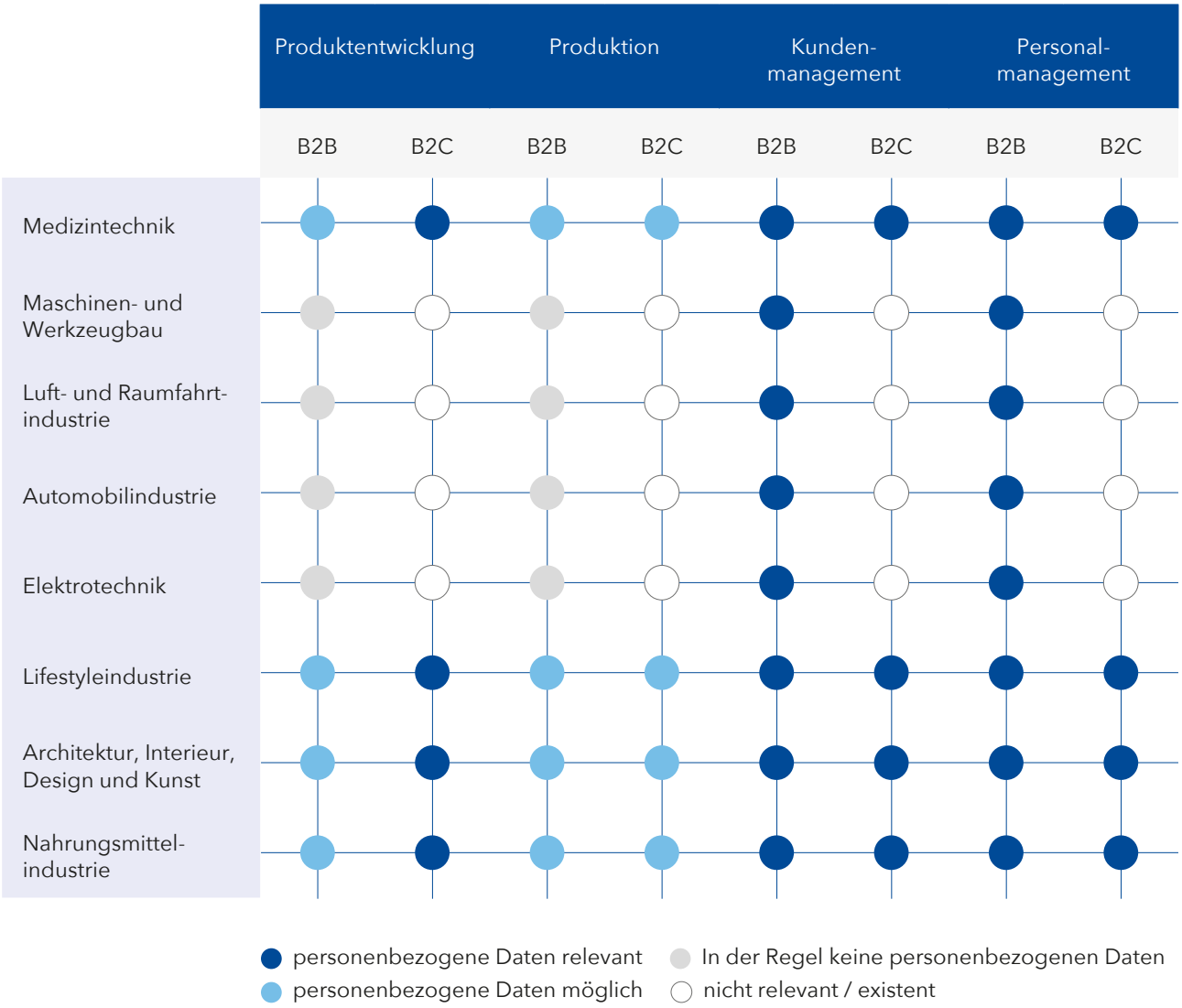


Tabelle 7: Relevanz von personenbezogenen Daten in der additiven Fertigung
Quelle: eigene Zusammenstellung atene KOM GmbH

4.5 Risiken bei der Verarbeitung von personenbezogenen Daten im Unternehmensprozess

4.5.1 Allgemeine Risiken bei der Datenverarbeitung

Mit der Verarbeitung personenbezogener Daten verpflichten sich Unternehmen zum Datenschutz im Rahmen der gültigen Gesetze. Eine Verletzung des Datenschutzes liegt vor, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ohne dass ein Gesetz dies erlaubt oder anordnet, oder der Betroffene in die jeweilige Erhebung, Verarbeitung oder Nutzung eingewilligt hat. Risiken entstehen immer dann, wenn die Vorgaben der DSGVO nicht eingehalten werden (siehe Kapitel 3). Dazu zählen beispielsweise unzweckmäßig gesammelte Daten, die nicht durch eine Einverständniserklärung der Nutzer abgedeckt werden, aber auch Sicherheitslücken im Unternehmen, die zur unautorisierten Verbreitung oder Verlust personenbezogener Daten führen.

Im Bereich der Informationssicherheit gibt es drei Grundsätze, die bei Nichtbeachtung zu Risiken für das Unternehmen führen können:[44]

- Vertraulichkeit: Personenbezogene Daten sind vertrauliche Informationen, die nur dem vorgesehenen Empfängerkreis zugänglich gemacht werden dürfen.
- Verfügbarkeit: Zum geforderten Zeitpunkt sollen personenbezogene dem Benutzer zur Verfügung stehen.
- Integrität: Die personenbezogenen Daten sind vollständig und unverändert.

Die negativen Konsequenzen durch falschen Umgang mit personenbezogenen Daten reichen von finanziellen Verlusten zu rechtlichen Sanktionen und Störung der Geschäftsbeziehungen. In vielen Fällen wird das Image des Unternehmens durch den Vertrauensverlust beschädigt. Auch die Handlungsfähigkeit des Unternehmens kann eingeschränkt werden.

Unrechtmäßige Erhebung oder nicht termingerechtes Löschen

Bei der Erhebung von personenbezogenen Daten gehen Unternehmen ein Risiko ein, wenn sie nach dem Prinzip „lieber zu viel als zu wenig" vorgehen. Art. 6 der DSGVO regelt die Rechtmäßigkeit der Verarbeitung personenbezogener Daten. Die erhobenen Daten sollten ausschließlich für den Zweck des Vertragsgegenstands benötigt werden und nicht darüber hinaus gehen. Jedes einzelne Datenfeld sollte begründet sein. Besondere Vorsicht ist bei sensiblen Daten geboten, die beispielsweise gesundheitliche oder finanzielle Informationen beinhalten.

Solange personenbezogene Daten gespeichert sind, gehen Unternehmen das Risiko ein, dass diese nicht termingerecht bzw. aufgrund einer Löschanfrage gelöscht werden.

Verlust / unbeabsichtigte Weitergabe durch Mitarbeiter und Dienstleister

Daten sind in Unternehmen über die gesamte Infrastruktur verteilt. Sie tauchen in verschiedenen Dokumenten wie E-Mails, Präsentationen und Verträgen auf und werden in unterschiedlichen Formen geteilt und weitergegeben. Es fällt Unternehmen oft nicht leicht, hier den Überblick zu bewahren. Dadurch entsteht die Gefahr der versehentlichen Weitergabe von personenbezogenen Daten.

In vielen Fällen entstehen Datenschutz-Risiken durch mangelhaftes Wissen und mangelnde Vorsicht der Mitarbeiter oder Dienstleister. Sensible Daten können dadurch unbewusst offengelegt werden und in die falschen Hände gelangen – etwa durch die Nutzung von unverschlüsselten USB Sticks, unsachgemäßes Kopieren und Entsorgen von Dokumenten, E-Mail-Anhänge, öffentlich zugängliche Passwörter, falsche Sicherheitseinstellungen oder unpassende Zugriffsrechte.

Die Weitergabe von Daten an Dritte kann auch durch den unsachgemäßen Einsatz von digitalen Diensten geschehen – etwa, wenn Buttons von sozialen Netzwerken auf der Website des Unternehmens eingebunden werden.

44 Bundesamt für Sicherheit in der Informationstechnik. (2012). Leitfaden Informationssicherheit. IT-Grundschutz kompakt. Abgerufen von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile

Fehlerhafte Daten
Personenbezogene Daten müssen als solche klassifiziert sein, korrekt zugeordnet und aktuell gehalten werden. Bei der Speicherung, Übermittlung und Verwaltung von Datensätzen können Fehler passieren. Als Folge können Daten durcheinandergeraten und den falschen Personen zugeordnet oder ganz gelöscht werden. Dadurch wird die Integrität der Daten gefährdet.

Bei der Erhebung besteht außerdem das Risiko, dass gefälschte Nutzerdaten übernommen werden. Im Laufe der Zeit ändern sich personenbezogene Daten und müssen entsprechend aktualisiert werden.

Diebstahl / nicht ausreichender Schutz vor unautorisiertem Zugang
Neben dem oftmals unbewussten Datenverlust müssen sich Unternehmen auf gezielte Angriffe und die Gefahr des Datendiebstahls einstellen. Die Methoden der Angreifer sind vielfältig und müssen mit einer Reihe von unterschiedlichen Maßnahmen wie Verschlüsselung, den aktuellsten Updates, Zwei-Wege-Authentifizierung, Viren-Scannern und Firewalls begegnet werden. Auch wenn es keine absolute Sicherheit gibt, können viele Angriffsoptionen durch relativ einfache Maßnahmen verhindert werden, wenn diese konsequent eingehalten werden.

Neben den digitalen Angriffsmöglichkeiten können Daten auch über den unbefugten Eintritt in die Unternehmensräumlichkeiten oder durch Mitarbeiter gestohlen werden.

Die erbeuteten personenbezogenen Daten können verkauft werden und bieten ein Erpressungspotenzial gegenüber Unternehmen, die mit einem Imageverlust und eventuell weiteren rechtlichen Konsequenzen rechnen müssen.

Sowohl im Falle eines unbeabsichtigten Verlusts als auch bei Diebstahl müssen Unternehmen vorbereitet sein und angemessen auf das Datenleck reagieren. Unternehmen gehen ein Risiko ein, wenn die Betroffenen nicht über den Vorfall informiert werden und keine effektiven Maßnahmen wie das Einspielen von Sicherheitsupdates ergriffen werden, um dem Vorfall zu begegnen.

4.5.2 Verarbeitungsrisiken im Unternehmensprozess der additiven Fertigung

Personenbezogenen Daten werden in einem Unternehmen in verschiedenen Prozessen und Schritten verarbeitet. Dies kann zum einen die firmeninterne Organisation betreffen und zum anderen die wirtschaftliche Betätigung. Die folgende Tabelle beschreibt diese Schritte im Unternehmen und zeigt auf, welche Risiken jeweils als besonders hoch einzuschätzen sind.

Prozesse / Schritte	Beschreibung	hohes Risiko
Personal-management	Personenbezogene Daten zu Mitarbeitern werden bei ihrer Einstellung oder bereits während ihrer Bewerbung aufgenommen. (z. B. CV, Kontodaten, Adresse). Im Laufe ihrer Anstellung kommen viele weitere Daten bezüglich ihrer Tätigkeit hinzu (z. B. Arbeitszeiten, Verdienst, Krankmeldungen).	• Verlust / unbeabsichtigte Weitergabe durch Mitarbeiter und Dienstleister • Diebstahl / nicht ausreichender Schutz vor unautorisiertem Zugang • Nicht termingerechtes Löschen
Dienstleister-management	Personenbezogene Daten zu Dienstleistern werden zu Beginn der Zusammenarbeit (z. B. im Rahmen der Vertragsschließung) sowie laufend während des Geschäftsbetriebs verarbeitet (z. B. im Rahmen der Kommunikation).	• Verlust / unbeabsichtigte Weitergabe durch Mitarbeiter • Diebstahl / nicht ausreichender Schutz vor unautorisiertem Zugang • Fehlerhafte Daten
Auftragserfüllung Auftragsaufnahme Zwecksbestimmung	Daten zu einem Kunden und zum gewünschten Produkt werden aufgenommen und zugeordnet. Die Daten für das Produkt können anhand verschiedener Kanäle übermittelt werden (Cloud, Webshop, USB, E-Mail etc.). Art und Umfang der personengebundenen Daten sind von verschiedenen Faktoren abhängig (siehe Kapitel 4.4). Im Regelfall werden mindestens Kontakt- und Rechnungsdaten angelegt und in einem CRM-System gespeichert.	• Unrechtmäßige Erhebung • Fehlerhafte Daten • Diebstahl / nicht ausreichender Schutz vor unautorisiertem Zugang
Datenaufbereitung	Aus den erfassten Daten zum gewünschten Produkt werden CAD-Daten erstellt, wenn diese noch nicht direkt übermittelt wurden.	• Diebstahl / nicht ausreichender Schutz vor unautorisiertem Zugang
Fertigung	Das gewünschte Produkt wird anhand der aufbereiteten Daten additiv gefertigt und anschließend nachbearbeitet.	• Diebstahl / nicht ausreichender Schutz vor unautorisiertem Zugang
Rechnungsstellung	Als Bestandteil der Rechnungsstellung werden Angaben wie Name und Anschrift von Aussteller und Empfänger, Rechnungsnummer, Preis und gelieferter Ware benötigt.	• Diebstahl / nicht ausreichender Schutz vor unautorisiertem Zugang • Verlust / unbeabsichtigte Weitergabe durch Mitarbeiter und Dienstleister
Zweckerfüllung	Nach Ablauf der Zweckerfüllung werden personenbezogene Daten gelöscht oder gesperrt.	• Nicht termingerechtes Löschen

Tabelle 8: Risiken im Unternehmensprozess der additiven Fertigung
Quelle: eigene Zusammenstellung atene KOM GmbH

5 HANDLUNGSEMPFEHLUNGEN FÜR KMU

An dieser Stelle soll geklärt werden, wie kleine und mittlere Unternehmen – einerseits branchenunabhängig und andererseits speziell Unternehmen aus dem Bereich der additiven Fertigung – ihre Unternehmensprozesse unter datenschutzrechtlichen Aspekten sicher gestalten können.

Datenschutz ist ein sehr individuelles Thema. Die Anforderungen und dementsprechend auch die zu ergreifenden Maßnahmen variieren je nach Größe des Unternehmens, nach Art und Menge der personenbezogenen Daten, sowie nach Verarbeitungsprozessen.

Handlungsempfehlungen zu diesem Thema sind daher nur bedingt allgemein gültig. Aus diesem Grund zeigen viele der folgenden Handlungsempfehlungen Möglichkeiten auf, die durch die Unternehmen entsprechend auf Relevanz und Umsetzbarkeit geprüft werden müssen.

5.1 Grundlegende Empfehlungen

Thema ernst nehmen – aber nicht in Panik verfallen

Die DSGVO wurde vor der Einführung am 25.05.2018 heiß diskutiert. Die mediale Aufmerksamkeit konzentrierte sich insbesondere auf das Thema Bußgelder, denn Datenschutzverstöße müssen in Zukunft geahndet werden. Zusätzlich verschiebt sich die Obergrenze der Strafen von 50.000 € bzw. 300.000 € in Ausnahmefällen auf max. 20 Mio. €. Durch die Meldepflicht werden die Aufsichtsbehörden außerdem wahrscheinlich häufiger von Datenschutzverletzungen erfahren.

Natürlich führten diese Ankündigungen zunächst zu Unruhe und Unsicherheit in Unternehmen. Besonders kleine Unternehmen mit eingeschränkten Kapazitäten und Ressourcen sahen in der DSGVO eine unüberwindbare Hürde. Dies spiegelt sich auch in einer repräsentativen Umfrage des Digitalverbandes Bitkom vom September 2017 wieder, in der nur etwa 30 % der Unternehmen angaben, die Vorgaben bis zum Mai 2018 voraussichtlich ungesetzt zu haben.[45]

Doch auch wenn die Anforderungen hoch erscheinen, darf man sich nicht abschrecken oder verunsichern lassen, denn grundsätzlich fallen in kleineren Unternehmen weniger Datenverarbeitungsvorgänge an und auch die Strukturen dürften übersichtlicher sein. Mit einer entsprechend guten Vorbereitung kommen KMU nicht in die Verlegenheit, sich mit Bußgeldern auseinandersetzen zu müssen. Dabei kann ein proaktiver Kontakt mit der zuständigen Datenschutzbehörde hilfreich sein, die ebenfalls beratende und unterstützende Funktionen erfüllt.

Herangehensweise festlegen

Im Hinblick auf das Inkrafttreten der DSGVO im Mai 2018 mussten und müssen sich Unternehmen aktiv mit dem Thema Datenschutz und Datensicherheit im Unternehmen auseinandersetzen. Die Herangehensweise kann sich dabei, je nach Kapazitäten und Prioritäten, unterscheiden: Soll lediglich das Nötigste erledigt werden, um den neuen Anforderungen zu genügen oder soll der Anlass genutzt werden, um die Daten- und IT-Sicherheit im Unternehmen grundlegend zu optimieren?

Bei einer ganzheitlichen Herangehensweise sollte die DSGVO als Chance verstanden werden: Alle datenrelevanten Prozesse werden überprüft und optimiert auch im Hinblick auf Unternehmensdaten und Risiken, die über eine Strafverfolgung und deren Konsequenzen hinausgehen. Dieser Ansatz greift auch bei Risiken außerhalb von Bußgeldern, Schadensersatzforderungen und schlechter Presse. Denn auch wenn es nicht zu einem angezeigten Gesetzesverstoß von Seiten des Unternehmens kommt, kann dieses bei unzulänglicher Datensicherheit Schaden nehmen, denkt man z. B. an Wirtschaftsspionage oder Erpressung.

Der risikobasierte Ansatz umfasst vor allem die Vermeidung von Bußgeldern, Schadensersatzforderungen und schlechter Presse. Es geht dabei darum, sich möglichst effektiv gegen Klagen von Verbrauchern, Verbraucheranwälten oder -verbänden sowie gegen Ermittlungen von Datenschutzbehörden zu verteidigen. Dies setzt vor allem ein professionelles Datenschutz-Management-System und

45 Bitkom. (2017, 19. September). Privacy Conference EU-Datenschutzgrundverordnung – Wie gut ist die deutsche Wirtschaft vorbereitet? Abgerufen 2. März, 2018, von https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/09-September/Privacy-Conference/Bitkom-Charts-PK-Privacy-Conference-19-09-2017-final.pdf

intelligente Dokumentations- und Kontrollprozesse voraus. Insbesondere hinsichtlich der umfassenden Betroffenenrechte, der erweiterten Dokumentationspflichten und der hohen Bußgeld- und Schadensersatzrisiken, konzentriert sich das Unternehmen bei dieser Herangehensweise auf das Wesentliche, anstatt zu versuchen jeglichen Anforderungen gerecht zu werden. Die Maßnahmen, die sich auf „das Wesentliche" konzentrieren, sind in Kapitel 5.3 beschrieben.

Informieren, Tools und Beratungsangebote nutzen

Es versteht sich von selbst, dass man zunächst die gesetzlichen Bestimmungen kennen sollte. Zum besseren Verständnis der Paragrafen und zur Einschätzung der eigenen Situation bieten sich Quellen an, welche die Informationen verständlich aufbereiteten.

Nicht nur die Bundesbeauftragte für Datenschutz und die Aufsichtsbehörden der Bundesländer standen den Unternehmen in der Vorbereitung sowie auch nach Inkrafttreten der DSGVO beratend zur Seite, auch verschiedene Organisationen und Verbände bieten Unterstützung an. Neben Informationsmaterial gibt es auch Tools wie Fragebögen, Selbsttests und Checklisten sowie Beratungsangebote und Handlungsempfehlungen. Um nicht den Überblick zu verlieren, ist folgend eine kleine Auswahl an Anlaufstellen und konkreten Angeboten aufgelistet:

Stelle / Angebot	Website
Bundesbeauftragte für Datenschutz	https://www.bfdi.bund.de/DE/Home/home_node.html
Hessischer Datenschutzbeauftragter	https://www.datenschutz.hessen.de/
Roadshow der DIHK und des BMWi	https://www.dihk.de/presse/meldungen/2018-01-18-road-show-datenschutz
Datenschutzkonferenz Kurzpapiere	https://www.bfdi.bund.de/DE/Home/-Kurzmeldungen/DSGVO_Kurzpapiere1-3.html
Fragebogen zur Umsetzung der DSGVO des bayerischen Landesamts für Datenschutzaufsicht	https://www.lda.bayern.de/media/-dsgvo_fragebogen.pdf
Online-Test „Weg zur DSGVO - Selbsteinschätzung	https://www.lda.bayern.de/tool/start.html
Informationen zum Verfahrensverzeichnis des Bitkom	https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/FirstSpirit-1496129138918170529-LF-Verarbeitungsverzeichnis-online.pdf

Tabelle 9: Tools, Informations- und Beratungsangebote
Quelle: eigene Zusammenstellung atene KOM GmbH

Mitarbeiter sensibilisieren und schulen

Schulungen zum Datenschutz stärken das Bewusstsein der Mitarbeiter für den Datenschutz. Dabei geht es im Wesentlichen darum, Risiken, die durch – oft unabsichtliches – Fehlverhalten entstehen, zu minimieren und die Mitarbeiter zu datenschutzkonformem Verhalten zu befähigen.

Zur Umsetzung sollte ein nachhaltiges Schulungskonzept erstellt werden, das sicherstellt, dass alle Personen geschult werden, die mit personenbezogenen Daten in Berührung kommen. Diese Schulungen vermitteln die Anforderungen der DSGVO für die unterschiedlichen Unternehmensbereiche und das passende Verhalten.

Die verschiedenen Mitarbeitergruppen im Unternehmen sollten dabei im Hinblick auf die Art der Daten sowie die Häufigkeit im Umgang mit personenbezogenen Daten berücksichtigt werden, z. B. Geschäftsleitung, Recht, IT, Finanzen, Forschung und Entwicklung oder Personalabteilung. In ein Schulungskonzept kann ebenfalls miteinfließen, ob bereits Vorkenntnisse bestehen. Dementsprechend können Grundschulungen und erweiterte Schulungen zu speziellen Themen angeboten werden.

Datenschutztrainings dienen als ergänzende Maßnahmen, um das theoretisch Gelernte anhand der Einübung konkreter Vorgänge und Prozesse besser in die Praxis übertragen zu können.

Eine besondere Rolle bei den Schulungen kommt dem betrieblichen Datenschutzbeauftragten zu: Einerseits ist es dessen Aufgabe, die Sensibilisierung und Schulung von Mitarbeitern zu überwachen. Andererseits ist es wichtig, dass der Datenschutzbeauftragte selbst in für die Rolle relevanten Themen fortlaufend intensiv geschult wird.

Projektteam und Datenschutzbeauftragter

Eine der ersten Herausforderungen wird es sein, das notwendige Bewusstsein im Unternehmen für die (neue) Bedeutung des Datenschutzes zu schaffen. Empfehlenswert ist hier, ein eigenes Projektteam aufzubauen, das mit der Umsetzung der DSGVO im Unternehmen betraut wird. Die Mitglieder dieses Projektteams sollten sich aus einem Unternehmensverantwortlichen, einem Mitarbeiter der IT, dem Rechts- und Compliancebereich (sofern vorhanden) und der Personalabteilung zusammensetzen.

Ein Datenschutzbeauftragter wird benötigt, sofern personenbezogene Daten automatisiert verarbeitet werden. Für kleine Betriebe gilt die Ausnahme, dass sich mindestens zehn Mitarbeiter regelmäßig mit personenbezogenen Daten beschäftigen müssen, damit ein Datenschutzbeauftragter benötigt wird. Dieser hat eine beratende sowie überwachende Funktion, schult die Mitarbeiter und ist offizieller Ansprechpartner, dessen Kontaktdaten veröffentlicht werden.

Es ist daher nicht empfehlenswert, einen beliebigen Mitarbeiter zum Datenschutzbeauftragten zu ernennen. Zur passenden Wahl eines Datenschutzbeauftragten sollten folgende Kriterien beachtet werden:

- Fachkunde: Juristisches Datenschutzwissen, IT-Fachwissen
- Charaktereigenschaften: Zuverlässig, gewissenhaft, durchsetzungsfreudig
- Verhaltensweise: Lernbereit, unparteiisch, vorbildlich
- Position im Unternehmen: keine Interessenkonflikte zwischen den Belangen des Datenschutzes und denen des Unternehmens – was beispielsweise bei der Geschäftsführung, oder dem Personal aus der IT-Abteilung regelmäßig der Fall ist

Datenschutzbeauftragte haften für Schäden, theoretisch auch mit dem Privatvermögen, wenn der Schaden absichtlich oder grob fahrlässig verursacht wurde. Um den Posten trotzdem zu vermitteln, könnten folgende Maßnahmen durchgeführt werden:

- Mitarbeiter und Unternehmen einigen sich auf eine schriftliche Vereinbarung zum Reduzieren der Haftungsrisiken
- Abschließen einer Berufshaftpflichtversicherung für den Datenschutzbeauftragten[46]
- Beauftragung eines externen Datenschutzbeauftragten

Externe Unterstützung?

Der Datenschutzbeauftragte muss kein interner Mitarbeiter sein, sondern kann auch extern in Person eines Dienstleisters bestellt werden. Der Vorteil eines internen Datenschutzbeauftragten ist, dass dieser das Unternehmen sowie die Geschäftsabläufe und verantwortliche Personen kennt. Demgegenüber bietet die Bestellung eines externen Datenschutzbeauftragten den Vorteil, dass dieser von außen objektiver auf das Unternehmen blicken und den Datenschutz unbefangen voranbringen kann.

46 Maenz, F. (2017, 14. Dezember). DSGVO & KMU: Was gibt es zu wissen für Datenschutzbeauftragte? [Blogeintrag]. Abgerufen 6. März, 2018, von https://blogs.business.microsoft.com/de-de/2017/12/14/die-dsgvo-und-die-rolle-des-datenschutzbeauftragten-in-kmu-kleinunternehmen-und-mittelstand/

Es bestehen neben dem externen Datenschutzbeauftragten weitere Möglichkeiten Hilfe von außen zu beanspruchen, z. B. durch Anwälte und Auditoren oder Berater. Eine repräsentative Umfrage des Digitalverbandes Bitkom[47] ergab, dass sich bislang etwa jedes zweite Unternehmen in Deutschland bei der Umsetzung der EU-Datenschutzgrundverordnung Hilfe von externen Experten geholt hat. Darunter fallen externe Anwälte (35 %), externe Prüfer oder Auditoren (29 %) sowie eine externe Datenschutzberatung (21 %).

Ob externe Unterstützung in Frage kommt, muss jedes Unternehmen individuell entscheiden und die Vor- und Nachteile unter Einbeziehung der intern zur Verfügung stehenden personellen und finanziellen Ressourcen abwägen.

47 Bitkom. (2017, 19. September).

5.2 Datenschutzmanagementsystem und Datenschutzkonzept

Begriffsabgrenzung

Begriffe wie Datenschutzmanagement, Datenschutzmanagementsystem, Datenschutzprozess und Datenschutzkonzept fallen immer wieder im Zusammenhang mit Datenschutz. Leicht kann es dabei zu Unklarheiten kommen, da die Begriffe häufig als Synonyme verwendet werden. Obwohl sie im Zusammenspiel miteinander stehen, sind die Begriffe voneinander abzugrenzen:

Unter **Datenschutzmanagement** sind übergeordnet alle Elemente und Prozesse zu verstehen, die notwendig sind, um die Umsetzung der gesetzlichen Anforderungen zu planen, zu organisieren, zu steuern, zu kontrollieren und damit sicher zu stellen. Datenschutzmanagement stellt somit die übergeordnete Umsetzung des Datenschutzes innerhalb eines Unternehmens dar. Das **Datenschutzmanagementsystem** ist entsprechend die Verbindung und das Zusammenspiel aller Elemente und Prozesse zu einer in sich schlüssigen Gesamtheit. Das System beinhaltet auch externe Elemente, die durch Prozesse mit dem internen Datenschutzmanagement verbunden sind, wie z. B. Kunden, Dienstleiter und Aufsichtsbehörden.

Die Erstellung eines **Datenschutzkonzeptes** ist ein Teil des Datenschutzmanagements. Ein Datenschutzkonzept legt fest, wie der Schutz der informationellen Selbstbestimmung der betroffenen Personen von dem verarbeitenden Unternehmen sichergestellt werden soll. Es beschreibt die notwendigen Informationen zum datenschutzkonformen Umgang mit personenbezogenen Daten und legt geeignete Maßnahmen fest.

Die Wirksamkeit der Maßnahmen sollte regelmäßig überprüft, bewertet, evaluiert und ggf. angepasst werden. Das bedeutet für Unternehmen und Datenschutzbeauftragte, dass sie ihr Datenschutzkonzept immer wieder überarbeiten müssen. Diesen sich wiederholenden Vorgang kann man als **Datenschutzprozess** beschreiben.

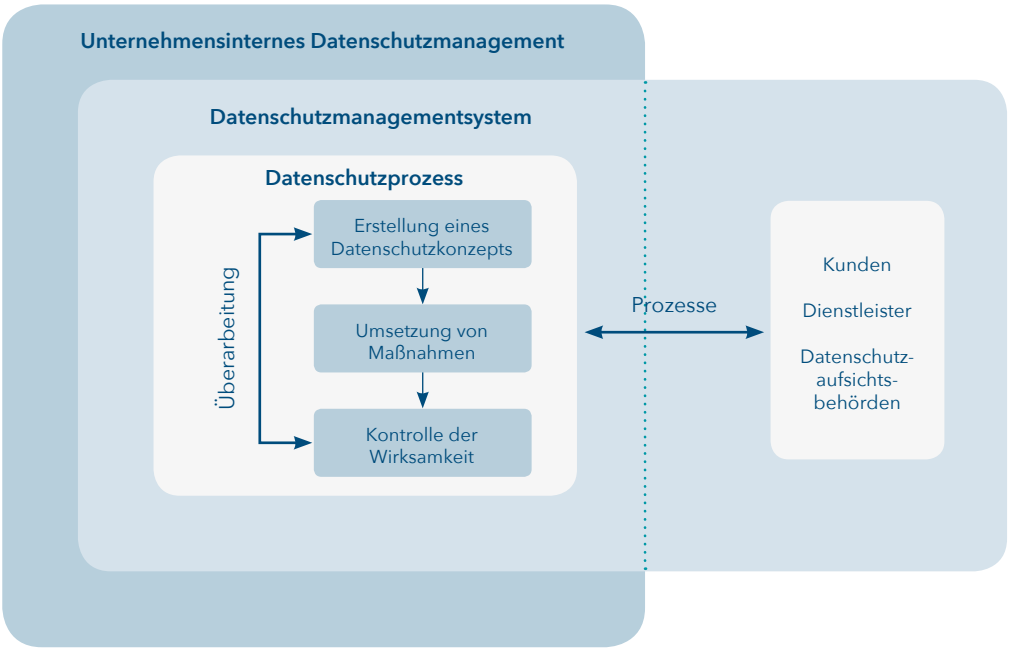


Abbildung 5: Elemente und Organisation des Datenschutz im Unternehmen
Quelle: Eigene Darstellung atene KOM GmbH

Einführen eines Datenschutzmanagementsystems

Um den Anforderungen der DSGVO gerecht zu werden, braucht jedes Unternehmen zwingend ein Datenschutzmanagementsystem, das den gesamten datenschutzkonformen Umgang mit personenbezogenen Daten regelt. Dies ist besonders auf Grund der neu eingeführten Rechenschaftspflicht der Fall. Damit sind nicht nur die Zuständigkeit und Verantwortung für die Einhaltung der festgelegten Prinzipien zur Datenverarbeitung zu verstehen, sondern auch eine Nachweispflicht. Das Unternehmen muss nachweisen können, dass es als Verantwortlicher angemessene und wirksame Maßnahmen ergreift, um die datenschutzrechtlichen Grundsätze und Verpflichtungen umzusetzen. Die Rechenschaftspflicht erstreckt sich auf alle Anforderungen, welche die Grundverordnung an den für die Verarbeitung Verantwortlichen stellt. Es empfiehlt sich daher, das Datenschutzmanagementsystem mit bereits im Unternehmen bestehenden Management- und Kontrollsystemen zu verknüpfen.

Besteht in einem Unternehmen bereits ein umfangreiches Informations-Sicherheits-Management-System (ISMS), im Bestfall sogar nach internationalen Standards (ISO/IEC 27001) zertifiziert, kann dieses um datenschutzrechtliche Aspekte erweitert werden. Informationssicherheit und Datenschutz sind zwar nicht deckungsgleich, denn ein ISMS behandelt alle zu schützenden Daten gleich und legt keinen Fokus auf personenbezogene Daten. Datenschutz ist jedoch ohne IT-Sicherheit nicht möglich, weshalb ein ISMS eine gute Grundlage bildet.

Es gibt eine Reihe von frei verfügbaren Orientierungshilfen und Anleitungen zur Implementierung eines Datenschutzmanagementsystems, beispielsweise von der Gesellschaft für Datenschutz und Datensicherheit.[48]

Mögliche Inhalte für ein Datenschutzkonzept

Das Datenschutzkonzept sollte alle im jeweiligen Unternehmen relevanten Datenschutzaspekte beinhalten und Grundlage eines jeden datenschutzrelevanten Handelns sein. Im Konzept werden die umfangreichen Ziele sowie weitere Punkte, die relevant für die Entwicklung der richtigen Strategien und Maßnahmen sind, beschrieben und festgelegt.

Ein Datenschutzkonzept ist keine Pflicht. Es wird dennoch empfohlen eines zu erstellen, da es die Organisation des Datenschutzes unterstützt und eine strukturierte Grundlage für regelmäßige Überprüfungen bietet. Zum Aufbau eines Datenschutzkonzeptes gibt es keine Vorschriften. Ein strukturierter Aufbau mit klarer Aufgabentrennung ist aber von Vorteil.

Gibt es in einem Unternehmen bereits ein Datenschutzkonzept, welches auf den bisherigen rechtlichen Anforderungen basiert, muss es an diesen Stellen überarbeitet und die Maßnahmen entsprechend angepasst werden.

Folgende Punkte sollten in einem Datenschutzkonzept Beachtung finden (zu einer Vielzahl der Punkte finden sich Beschreibungen und Empfehlungen zur Umsetzung in den Kapiteln 5.3 und 5.4):

- Definitionen / Begrifflichkeiten
- Zielsetzung und Gültigkeitsbereich
- Datenschutz- und Sicherheitspolitik des Unternehmens
- Akteure / Beteiligte und Verantwortlichkeiten im Unternehmen
- Rechtliche Grundlagen / Vorgaben
- Zu verarbeitende Daten und ihr Schutzbedarf
- Datenschutzbezogene Anforderungen
- Führung des Verzeichnisses von Verarbeitungstätigkeiten
- Regelungen für den Fall der Auftragsverarbeitung
- Betroffenenrechte und Transparenz der Datenverarbeitung
- Risikobewertung
- Datenschutz-Folgenabschätzungen
- Meldung von Verletzungen des Datenschutzes
- Technisch-organisatorische Datenschutzmaßnahmen (TOM)
- Datenschutz-Schulungen
- Kontrollen / Überprüfungen / Audits

Die Umsetzung eines Datenschutzkonzeptes sollte im Rahmen eines klassischen Projektmanagements mit einem Projekt- und Arbeitsplan erfolgen.

48 Gesellschaft für Datenschutz und Datensicherheit e.V. (2016). GDD-Praxishilfe DS-GVO III. To-Dos für die Übergangsfrist bis zur Geltung der DS-GVO. Abgerufen von https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_3.pdf

5.3 Empfehlungen zur Anpassung an die Änderung durch die DSGVO

Die in Kapitel 3 beschriebenen Änderungen, die sich durch die Wirksamkeit des Inkrafttretens der DSGVO ergeben, stellen KMU vor konkrete Herausforderungen (vgl. Tabelle in Kapitel 3.9). Die folgenden Empfehlungen sollen KMU dabei unterstützen, diese Herausforderungen zu meistern.

5.3.1 Anwendungsbereich

Bestandsaufnahme durchführen
Um den Anwendungsbereich in einem Unternehmen identifizieren zu können, sollte bekannt sein, welche Prozesse und Verfahren zur Verarbeitung personenbezogener Daten im Unternehmen überhaupt bestehen. Denn diese Verfahren bilden die Grundlage, auf der die Anpassungen an die DSGVO aufgebaut werden sollten.

Hierzu empfiehlt sich zunächst eine Übersicht aller im Unternehmen eingesetzten Anwendungen und Tools (IT-Verfahren und Dateien) zu erstellen, in denen personenbezogene Daten verarbeitet werden. Typische Beispiele sind Zeiterfassungssysteme, E-Mailverarbeitungen, CRM-Systeme, Personalverwaltung und Websitebesucheranalysen.

Die Informationen können, je nach Größe des Unternehmens, durch eine zuständige Person recherchiert oder durch Einbeziehung der verschiedenen Abteilungen oder Teams abgefragt werden. Das Ergebnis könnte in der Personalabteilung z. B. folgende Verfahren beinhalten: Bewerbungsprozess, Arbeitsverträge, Lohnabrechnung, Krankheitsregelungen, Urlaub, Reisekosten, Zeiterfassung, Einsatz- und Arbeitsplanung, Versicherungen, etc. In der Rechtsabteilung hingegen ginge es hauptsächlich um die Vertragsgestaltung und die Buchhaltung wird vor allem bei der Rechnungstellung und Abrechnung personenbezogene Daten verarbeiten. Auf die Verarbeitung von Daten von Kindern sollte besonders genau geachtet werden.

Am Ende sollte dabei eine Übersicht mit allen personenbezogenen Daten stehen, die vom Unternehmen selbst oder von Dritten im Auftrag verarbeitet werden.

5.3.2 Betroffenenrechte

Datenschutzerklärungen und -informationen
Wann immer ein Unternehmen mit personenbezogenen Daten von Betroffenen umgehen möchte, muss der Betroffene in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache im Vorhinein darüber informiert werden.

Alle bestehenden Dokumente zur Erfüllung der Informationspflichten im Hinblick auf die Anforderungen der DSGVO müssen überarbeitet werden. Fehlende Dokumente müssen neu erstellt werden, dazu gehören z. B.:

- Datenschutzerklärung Webauftritte
- ggf. weitere Datenschutzerklärungen
- Information für Mitarbeiter (Datenverarbeitung im Arbeitsverhältnis)
- Information für Bewerber (Datenverarbeitung im Bewerbungsprozess)
- Information für Kunden (Datenverarbeitung im Produktionsprozess)
- Information für Auftragsdatenverarbeiter

Die Informationen sollten enthalten:
- Zweck der Verarbeitung
- Name und Kontaktdaten des Verantwortlichen und ggf. des Datenschutzbeauftragten
- Empfänger, falls Daten weitergegeben werden sollen
- Dauer der Speicherung, Kriterien für die Löschung
- Hinweise über Recht auf Auskunft, Löschung, Widerrufung

Prozess für Betroffenenanfragen
Das Recht auf Auskunft ist nichts Neues und ein entsprechender Prozess zur Bearbeitung von Anfragen sollte in jedem Unternehmen bereits bestehen. Eine Auskunft ist nur zu erteilen, wenn ein konkreter Antrag vorliegt.

Die Informationen müssen den Zweck, die Kategorie, den Empfänger von Daten und die geplante Speicherdauer enthalten. Es müssen die konkreten Inhalte genannt werden, nicht nur welche Art von Daten vorliegen, damit der Betroffene diese auf Richtigkeit überprüfen kann.

Da dem Antragsteller keine Kopie, sondern nur eine Abschrift zukommt, ist es ratsam eine Vorlage / Template für die schnelle und komplette Auskunft zu erstellen.

5.3.3 Dokumentation

An dieser Stelle sei noch einmal auf den Paradigmenwechsel, den der Gesetzgeber mit der DSGVO vorgenommen hat, hingewiesen: Bisher mussten Verstöße gegen geltendes Datenschutzrecht von der Aufsichtsbehörde belegt werden. Zukünftig muss das Unternehmen belegen können, dass es die Vorschriften der DSGVO eingehalten hat. Ist das Unternehmen nicht in der Lage, die Datenschutzkonformität seines Handelns zu belegen, liegt damit bereits ein bußgeldbewehrter Verstoß vor!

Die DSGVO trifft keine Aussagen darüber, wie eine Dokumentation aussehen soll. Die nachfolgende Abbildung kann als Orientierungshilfe dienen, welche Dokumente Teil einer lückenlosen Dokumentation sein könnten.

Abbildung 6: Mögliche Elemente der Datenschutzdokumentation
Quelle: Eigene Darstellung nach Lepperhoff & Müthlein (2017)

Verzeichnis von Verarbeitungstätigkeiten
Auch wenn Unternehmen mit weniger als 250 Mitarbeitern von dieser Verpflichtung freigestellt sind, spielt dies in der Praxis fast keine Rolle, denn auch KMU unterliegen umfassenden Dokumentationspflichten. Daher ist es sinnvoll, sich an den Vorgaben des Art. 30 DSGVO zu orientieren, denn eine Dokumentation des Datenschutzes wird in Streitfällen eine wichtige Rolle spielen. Ohne ein solches Verzeichnis ist die Anpassung der eigenen Prozesse an die DSGVO schwierig.

Das Verzeichnis von Verarbeitungstätigkeiten sollte schriftlich oder elektronisch angelegt werden und alle Prozesse berücksichtigen, in denen mit personenbezogenen Daten umgegangen wird, sowie weitere allgemeine Daten wie Kontakt und Zweck der Verarbeitung.

Auf Grundlage einer Bestandsaufnahme (vgl. 5.3.1) ist festzustellen, wie und auf welcher Rechtsgrundlage diese Daten übermittelt wurden, warum diese Daten gesammelt werden und wie lange sie gespeichert werden. Dafür ist es notwendig, dass die datenverarbeitenden Prozesse abteilungsübergreifend beschrieben werden, der Zweck der Datenverarbeitung für jedes einzelne Datenfeld festgehalten wird, eine Rechtsgrundlage für jedes Datenfeld und eine Löschfrist je Datenfeld festgelegt werden.

In der Folge sind die identifizierten Datenverarbeitungsvorgänge auf Vereinbarkeit mit der DSGVO zu prüfen. In der Regel dürfte sich dabei herausstellen, dass jedes Unternehmen die Datenmenge reduzieren und die Anzahl der Personen, die auf sie zugreifen dürfen, eingrenzen muss. Gegebenenfalls muss eine Einwilligung zur Nutzung der Daten von den Betroffenen eingeholt werden.

Anleitungen zur Erstellung von Verzeichnissen zur Verarbeitungstätigkeit sowie Beispiele und Muster stehen kostenlos im Internet zur Verfügung.[49]

5.3.4 Auftragsdatenverarbeitung

Verträge anpassen
Sinnvoll ist es, zunächst alle eingesetzten Dienstleister aufzulisten und zu prüfen, ob eine Berührung mit personenbezogenen Daten stattfindet, bzw. auch nur möglich ist. Mit der Einhaltung der DSGVO sind alle Personen zu verpflichten, die Zugang zu personenbezogenen Daten haben; hierzu gehören auch Dienstleister und Personen, die beispielsweise Einblick erhalten können. Wie bisher muss mit den Auftragsverarbeitern ein Vertrag über die „Datenverarbeitung" geschlossen werden. Etwaige bestehende Verträge müssen an die DSGVO angepasst werden – zwar entsprechen die Vorgaben aus der DSGVO weitestgehend denen aus dem bisher geltenden BDSG, es gibt aber einige Anforderungen, die ergänzt werden müssen, so z. B. die Dokumentationspflicht für Weisungen.

Die Erstellung neuer Vertragstemplates für neue Auftragsverarbeitungsverträge nach DSGVO ist empfehlenswert.

Sofern ein KMU selbst als Dienstleister und Auftragsverarbeiter fungiert, macht es das neue Haftungsszenario notwendig, sich bereits vor Auftragsübernahme mit den datenschutzrechtlichen Aspekten der zu übernehmenden Tätigkeit vertraut zu machen und entsprechende datenschutzrechtliche Maßnahmen zu etablieren. Darüber hinaus ist die übernommene Auftragsverarbeitung zu dokumentieren.

5.3.5 Datenschutz-Folgenabschätzung (DFSA)

Eine DSFA bezieht sich auf einzelne, konkrete Verarbeitungsvorgänge, für die vor Beginn einer geplanten Datenverarbeitung eine Abschätzung der Folgen der Verarbeitungsvorgänge für den Schutz personenbezogener Daten vorzunehmen und zu dokumentieren ist.

Für jede Verarbeitung ist mittels einer systematischen Risikobewertung zu klären, ob eine Datenschutz-Folgenabschätzung durchgeführt werden muss. Das Ergebnis ist zu dokumentieren (z. B. im Verzeichnis von Verarbeitungstätigkeiten). Für mehrere ähnliche Verarbeitungsvorgänge reicht eine Abschätzung, sofern diese ein ähnlich hohes Risiko haben.

Die Bewertung wird anhand von Kriterien durchgeführt, die für ein hohes Risiko für die Rechte und Freiheiten einer natürlichen Person sprechen. Es wird die Nutzung folgender Kriterien empfohlen, die von der Artikel-29-Datenschutzgruppe[50] vorgeschlagen werden:

- Scoring / Profiling
- Automatische Entscheidungen, die zu rechtlichen Folgen für die Betroffenen führen
- Systematische Überwachung
- Sensible Daten (besondere personenbezogene Daten aus Art. 9 DSGVO)
- Daten die in großem Umfang verarbeitet werden (Kriterium: Anzahl der Betroffenen, Menge der Daten etc.)
- Zusammenführen / Kombinieren von Daten die durch unterschiedliche Prozesse gewonnen wurden
- Daten geschäftsunfähiger oder beschränkt geschäftsfähiger Betroffener
- Einsatz neuer Technologien oder biometrischer Verfahren
- Datentransfer in Länder außerhalb der EU / EWR
- Die Datenverarbeitung hindert Betroffene an der Rechtsausübung

Für den Fall, dass mehr als ein Kriterium für die Datenverarbeitungsvorgänge zutrifft, wird empfohlen, eine DSFA durchzuführen.

49 Bitkom. (2017). Das Verarbeitungsverzeichnis Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 EU-Datenschutz-Grund verordnung (DS-GVO). Abgerufen von https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/FirstSpirit-1496129138918170529-LF-Verarbeitungsverzeichnis-online.pdf; Gesellschaft für Datenschutz und Datensicherheit e.V. (2016).

50 http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358

Die Bewertung des Risikos berücksichtigt je nach Verfahren die Eintrittswahrscheinlichkeit und die Schwere des Schadens (dies sind laut DSGVO z. B. Diskriminierung, Identitätsdiebstahl, Rufschädigung oder finanzieller Verlust)

Die DSGVO legt den Mindestinhalt einer Datenschutz-Folgenabschätzung wie folgt fest:

- Systematische Beschreibung der Verarbeitungsvorgänge und Zwecke
- Notwendigkeit und Verhältnismäßigkeit der Verarbeitung im Verhältnis zum Zweck der Verarbeitung
- Risikobewertung
- Geplante Abhilfemaßnahmen zur Bewältigung der Risiken

Verbleibt ein hohes oder sehr hohes Restrisiko, muss die zuständige Datenschutzaufsichtsbehörde konsultiert werden und deren Entscheidung (z. B. Einsatz nur nach Ergreifung weiterer Schutzmaßnahmen, Verbot der geplanten Verarbeitung) beachtet werden.

Die Durchführung einer Risikobewertung, das Ergebnis der Analyse und einer daraus ggf. abzuleitenden Datenschutz-Folgenabschätzung müssen gut dokumentiert sein, um der Rechenschaftspflicht nachzukommen.

5.3.6 Technische und organisatorische Maßnahmen

Geeignete technische und organisatorische Maßnahmen (TOM) müssen geplant, umgesetzt und dokumentiert werden, um sicherzustellen, dass die Verarbeitung gemäß den Vorgaben der Verordnung erfolgt und der Nachweis dafür erbracht werden kann.

Die Auswahl der TOM erfolgt auf Grundlage der Datenschutz-Folgenabschätzung bzw. der Risikobewertung und deren Ergebnis.

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. hat eine Kurzvorlage zur Dokumentation zu den TOM veröffentlicht, an der man sich gut orientieren kann.[51] Folgend ist kurz erklärt was mit den Begriffen gemeint ist und es werden Beispiele für Maßnahmen aufgelistet, die in Betracht gezogen werden können:

51 Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. (o.D.). Technische und organisatorische Maßnahmen gem. Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g) und Auftragsverarbeiter (Art. 30 Abs. 2 lit. d). Abgerufen 1. März, 2018, von https://www.bvdnet.de/wp-content/uploads/2017/06/Muster_Verz_der_Verarbeitungst%C3%A4tigkeiten_TOMs.pdf

Zweck	Bedeutung	Beispielmaßnahmen
Pseudonymisierung	Zuordnung eines Datums zu einem nicht personenbezogenen Namen, einer Nummer o.ä., welches eine Zuordnung erschwert	• Nutzen von Pseudonymen • Getrennte Aktenschränke • Getrennte Datenbanken
Verschlüsselung	Informationen werden mit Hilfe eines kryptografischen Verfahrens in eine nicht zu entschlüsselnde Zeichenfolge verwandelt	• Verschlüsselungsverfahren nach dem Stand der Technik • Verschlüsselung von Passwörtern
Gewährleistung der Vertraulichkeit	Kontrolle von Zutritt, Zugang und Zugriff bzw. Verhinderung von unbefugter oder unrechtmäßiger Verarbeitung	• Bauliche Maßnahmen • Zugangskontrollen • Zugriffsrechte • Alarmanlagen
Gewährleistung der Integrität	Daten sollen stets richtig und verlässlich sein und dürfen nicht unbeabsichtigt oder schadhaft geändert oder zerstört werden können	• Datensicherung / Backups • Prüfsummen • Virenscanner • Firewalls • Software-Updates
Gewährleistung der Verfügbarkeit	Systeme sollen bestmöglich gegen innere und äußere Einflüsse geschützt werden	• Abgesicherte Stromanschlüsse • Unterbrechungsfreie Stromversorgung(USV) • Blitzableiter
Gewährleistung der Belastbarkeit der Systeme	Systeme müssen auch kurzfristiger starker Beanspruchung die angeforderten Daten liefert sowie externe Angriffe überstehen	• Skalierende Systeme • Denial of Service – Abwehrtechniken • RAID-Systeme
Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall	Reaktion auf Zwischenfälle, um Daten bzw. den Zugang zu diesen schnellstmöglich wiederherzustellen	• Back-up-Systeme • Wiederherstellungsverfahren • Vertretungspläne für Personal • Notstromversorgung • Konkrete Notfallpläne • Gespiegelte Datenbanken oder redundante Server
Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen	Kontrolle aller TOM in regelmäßigen Abständen (Empfehlung mind. in jährlichen Abständen)	• Regelmäßige intern oder extern protokollierte Prüfungen • Evaluierungen durch Betroffene & Nutzer • Penetrationstests • Skalierbarkeit von Systemen

Tabelle 10: Technische und organisatorische Maßnahmen
Quelle: eigene Zusammenstellung atene KOM GmbH

5.3.7 Meldepflicht

Meldeprozesses
Es ist dringend zu empfehlen, dass Handlungsanweisungen etabliert werden, die eine unverzügliche Meldung aller Datenschutzverstöße einschließlich etwaiger Verdachtsfälle an einen Verantwortlichen (Datenschutzbeauftragter, Unternehmensverantwortlicher) vorsieht.

Der Prozess muss sicherstellen, dass möglichst binnen 72 Stunden ab Kenntniserlangung jeder relevante Vorfall an die Aufsichtsbehörde gemeldet werden kann und auch unternehmensintern publik gemacht wird. Die Meldung sollte folgende Punkte umfassen:

- Art der Verletzung
- Kategorien und ungefähre Zahl der Betroffenen und der Datensätze
- Name und Kontakt des Datenschutzbeauftragten
- Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung
- ergriffene und vorgeschlagene Maßnahmen zur Behebung

Die Aufsichtsbehörden stellen, für eine Meldung von Datenverletzungen, ein Internetbasiertes Formular zur Verfügung.

Zudem ist eine Sensibilisierung und Schulung der Mitarbeiter zu den Grundlagen des Datenschutzes unerlässlich – nur so werden die Mitarbeiter in die Lage versetzt, überhaupt eine potenzielle Datenschutzpanne zu erkennen. Dies betrifft auch die durchzuführende Risikoabwägung im Hinblick auf die Benachrichtigungspflicht gegenüber den Betroffenen. Im Fall, dass hier eine Benachrichtigung notwendig ist, müssen Angaben über die Art der Verletzung, die wahrscheinlichen Folgen sowie die zur Behebung ergriffenen oder vorgeschlagenen Maßnahmen enthalten sein. Die Erstellung von Templates zur Benachrichtigung ist empfehlenswert.

5.4 Spezifische Handlungsempfehlungen für KMU der additiven Fertigung

Im Bereich der additiven Fertigung werden meist Produktions- und Fertigungsdaten verarbeitet. Dennoch betreffen die Datenschutzregelungen wichtige Bereiche dieser Unternehmen wie z. B. Kundendaten und Mitarbeiterdaten. Bei einigen Unternehmen fließen personenbezogene Daten natürlicher Personen auch direkt in die additive Fertigung ein, wie etwa bei der individualisierten Produktion von Sportgeräten, medizinischen Prothesen oder dem 3D-Druck von Miniatur-Figuren als Ebenbild.

Die allgemeinen Aufgaben und entsprechende Handlungsempfehlungen, die jedes kleine und mittelständige Unternehmen unabhängig ihrer Tätigkeit betreffen, wurden bereits in den vorherigen Kapiteln betrachtet. Die folgenden Handlungsempfehlungen sind hauptsächlich Vertiefungen oder Ergänzungen der vorherigen Empfehlungen und richten sich konkret an Unternehmen aus der additiven Fertigung und orientieren sich an den typischen Prozessen und Vorgehensweisen in dieser Branche.

In der Praxis der additiven Fertigung haben einige Herstellerfirmen bereits einen besonderen Umgang mit personenbezogenen Daten eingeübt. Bei Auftraggebern insbesondere aus der Rüstungsindustrie, aber auch aus der Automobilbranche im Zusammenhang mit dem Prototypenbau oder Kleinserienfertigung ist es üblich, dem Unternehmen der additiven Fertigung Datenschutzklauseln im Vertrag vorzuschreiben. Wer solche Vorgaben als Maßstab auch für die Verarbeitung der Daten anderer Kunden exemplarisch heranzieht und anwendet, ist in der Regel auf der sicheren Seite.

Klassifikation der Daten nach Schutzstufen

Die Vorstufe einer Risikoanalyse ist eine Schutzbedarfsaufwendigfeststellung der zu verarbeitenden personenbezogenen Daten anhand der Datenarten (Kundendaten, Mitarbeiterdaten, Steuerdaten, Gesundheitsdaten etc.). Dadurch wird auch das Schadenspotenzial dieser Daten bestimmt. Diese Maßnahme erleichtert eine Priorisierung und angemessene Gestaltung der technischen und organisatorischen Schutzmaßnahmen. Eine Klassifikation ist gerade bei Daten wichtig, die eine besondere Kategorie im Sinne der DSGVO darstellen und aus denen beispielsweise Rückschlüsse über die ethnische Herkunft oder Gesundheitsdaten möglich ist.

Zur Klassifikation eignet sich beispielsweise das Schutzstufenkonzept der Landesbeauftragten für den Datenschutz Niedersachsen.[52] Dieses stellt fünf Stufen auf, die personenbezogene Daten erhalten können. In der höchsten Schutzstufe werden Daten verarbeitet, deren unsachgemäße Handhabung Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen könnte.

Auch wenn Daten mit dieser Schutzstufe in der additiven Fertigung vermutlich nicht erreicht werden, sind Daten mit möglichen Rückschlüssen auf die Gesundheit keine Seltenheit. Nach dem genannten Schutzstufenkonzept kann die unsachgemäße Handhabung dieser Daten „den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen". In der additiven Fertigung fallen entsprechende Daten etwa bei der Produktion von medizinischen Prothesen an.

Verschlüsselung und Pseudonymisierung der Druck-/Fertigungsaufträge

Es ist zu erwarten, dass insbesondere der B2C-Bereich eine wachsende Rolle in der additiven Fertigung einnehmen wird. Dies bedeutet, dass Fertigungsdaten vermehrt direkt vom Kunden mittels Konfiguratoren erstellt werden oder vom Kunden via verschiedener Kanäle übermittelt werden. Die Verschlüsselung der Daten sollte bereits bei der Übermittlung der Daten vom Kunden erfolgen, in entschlüsselter Form sollten sie nur autorisiertem Personal zur weiteren Bearbeitung zur Verfügung stehen.

Um ein angemessenes Schutzniveau zu erreichen, müssen Fertigungsaufträge für den Produktionsprozess pseudonymisiert werden. So können die Mitarbeiter in der Produktion keinen Bezug mehr zwischen Produkt und Kunde herstellen.

Umgang mit Auftragsverarbeitern

Viele Unternehmen der additiven Fertigung treten nicht nur selbst als Auftragsverarbeiter auf, sondern bedienen sich der Zu- und Mitarbeit anderer Dienstleister. Insbesondere bei der Übernahme von Kundendaten ist die Datenübermittlung über externe Plattformbetreiber und IT-Dienstleister ein wesentlicher Bestandteil der Verarbeitung. Diese Übermittlung passiert nicht selten über Cloud-Speicher. Damit in der Übermittlung keine Sicherheitsprobleme und Datenschutzlücken entstehen, sollten Cloud-Anbieter mit entsprechender Zertifizierung gewählt werden.

Zugleich sollten Unternehmen mit den Auftragsverarbeitern entsprechende Bestimmungen zum Datenschutz ausarbeiten. Es sollten zudem nur Auftragsverarbeiter gewählt werden, welche Verarbeitung nach Anforderungen der DSGVO durchführen und den Schutz der Daten gewährleisten können.

Löschen von Daten

Als gelöscht gelten Daten, wenn sie unkenntlich gemacht wurden.

Durch die Entwicklung und Herstellung individueller Produkte und Prototypen haben viele Unternehmen der additiven Fertigung häufig mit Geheimhaltungsvereinbarungen zu Konstruktionsdaten zu tun und werden explizit dazu aufgefordert, etwa durch Patent geschützte oder der Geheimhaltung unterliegende Daten zu löschen. Solche Vereinbarungen und Prozesse sind auf personenbezogene Daten auszuweiten.

Die generellen Vorgaben des Datenschutzes gelten natürlich auch hier: Während eine direkte Kundenbeziehung anhält, dürfen dessen Daten verarbeitet und aufbewahrt werden. Kunden, mit denen länger kein Kontakt bestanden hat, müssen dagegen in der Regel nach einem Jahr kontaktiert werden, wenn ihre Zustimmung zur weiteren Speicherung der Daten einzuholen ist. Die meisten CRM-Systeme verfügen über Routinen zur geplanten Löschung von Daten nach einer festzulegenden Frist oder andauernder Inaktivität.

52 Die Landesbeauftragte für den Datenschutz Niedersachsen. (2010, Oktober). Schutzstufenkonzept des LfD Niedersachsen. Abgerufen 1. März, 2018, von https://www.lfd.niedersachsen.de/technik_und_organisation/schutzstufen/schutzstufen-56140.html

Informationspflicht nachkommen
In Kapitel 5.3.2 wurden bereits einige Datenschutzinformationen aufgezeigt, die dem Betroffenen zur Verfügung gestellt werden müssen. Hier sollte besonderes Augenmerk auf den Umfang gelegt werden, in welchem die Daten zur additiven Fertigung benötigt werden. Dabei sollte auf das „Wie" der Datenverarbeitung eingegangen werden. Hinweise darauf, welche personenbezogenen Daten über den eigentlichen Kundenkontakt hinaus an welcher Stelle der Verarbeitung eine Rolle spielen, sollten dem Empfänger klar kommuniziert werden. Es muss nicht jede einzelne Instanz der Daten benannt werden, aber der Hinweis, dass auch die Konstruktionsdaten in der Verarbeitung möglicherweise einen Personenbezug erlauben, kann hilfreich sein.

5.5 Aktionsplan / Checkliste

Die folgende Checkliste sollte ein Vademecum, ein ständiger Begleiter der Datenschutz- und Informationssicherheitsverantwortlichen in den Unternehmen der additiven Fertigung sein. Dokumentation und Transparenz sind keine einmalige Aktivität, sondern müssen zu den ständigen betrieblichen Aufgaben gehören. Unternehmen sind den Anforderungen des Datenschutzes nur gewachsen, wenn sie ihre Mitarbeiter einbinden. Deshalb gehört die Sensibilisierung und Schulung all derer, die mit personenbezogenen Daten arbeiten, zum Grundbedarf jeder Maßnahme.

Maßnahmen	Einzelschritte	Ziel der Maßnahme
Datenschutzfolgenabschätzung (DSFA)	• Team, Prüfplanung, Scope, Akteure und Betroffene definieren • Bewertung von Notwendigkeit und Verhältnismäßigkeit • Rechtsgrundlagen identifizieren • Risikoquellen modellieren, Risiken beurteilen, Abhilfemaßnahmen auswählen • Umsetzung und Tests, Dokumentation, Freigabe • Audit und Fortschreibung	Systematische Risikoeindämmung, Verständnis der eigenen Prozesse bei der Verarbeitung personenbezogener Daten herstellen, Pflichten umsetzen
Auftragsverarbeiter / Plattformen / Cloud-Anbieter vertraglich binden	• Verträge in beide Richtungen prüfen • Als Auftragnehmer Datenschutz vertraglich zusichern • Von Dienstleistern Datenschutz garantieren lassen	Schaffung rechtssicherer Beziehungen zu Dienstleistern, Vertrauensbasis sichern
Technische und organisatorische Maßnahmen	• Technische IT-Sicherheit • Physische IT-Sicherheit (Zugangskontrollen) • Mitarbeiterschulungen • Meldekette • Zertifizierung	Eigen- und Fremdschutz absichern, Frühwarnsysteme etablieren

6 QUELLEN

Studien / Publikationen

Astor, M.; von Lukas, U.; Jarowinsky, M. et al. (2013). Marktperspektiven von 3D in industriellen Anwendungen. Abgerufen von https://www.prognos.com/uploads/tx_atwpubdb/130117_Prognos_IGD_MC_Studie_3D_Maerkte.pdf

Berger, U., Hartmann, A., & Schmidt, D. (2013). Additive Fertigungsverfahren. Rapid Prototyping, Rapid Tooling, Rapid Manufacturing. Haan-Gruiten: Verlag Europa-Lehrmittel. Abgerufen von https://www.europa-lehrmittel.de/downloads-leseproben/50335-1/269.pdf/

Bitkom. (2017). Das Verarbeitungsverzeichnis. Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 EU-Datenschutz-Grundverordnung (DS-GVO). Abgerufen von https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/FirstSpirit-1496129138918170529-LF-Verarbeitungsverzeichnis-online.pdf

Brockhausen, C. (2017, 4. September). Datenschutz: Das optimale „Privacy Impact Assessment" nach der DSGVO. Compliance Praxis, 19(3). Abgerufen von http://www.compliance-praxis.at/Fachartikel/Datenschutz-Das-optimale-Privacy-Impact-Assessment-nach-der-DSGVO/(shareHash)/9dbeb0f273f311c05dae24e179df8e1c

Bundesamt für Sicherheit in der Informationstechnik. (2012). Leitfaden Informationssicherheit. IT-Grundschutz kompakt. Abgerufen von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile

Caviezel, C., Grünwald, R., Ehrenberg-Silies, S., Kind, S., Jetzke, T., & Bovenschulte, M. (2017). Additive Fertigungsverfahren (3-D-Druck) (Arbeitsbericht Nr. 175). Abgerufen von http://www.tab-beim-bundestag.de/de/pdf/publikationen/berichte/TAB-Arbeitsbericht-ab175.pdf

Deutscher Bundestag. (2017). Technikfolgenabschätzung (TA) Additive Fertigungsverfahren „3-D-Druck" (Bericht des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung (18. Ausschuss) gemäß § 56a der Geschäftsordnung). Abgerufen von http://dip21.bundestag.de/dip21/btd/18/134/1813455.pdf

Eßer, M., Kramer, P. & Lewinski, K. V. (2017). DSGVO BDSG (5. Aufl.). Carl Heymanns Verlag.

Europäische Kommission. (2003). Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (2003/361/EG). Abgerufen von http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32003H0361&from=DE

Expertenkommission Forschung und Innovation (2015). Additive Fertigung („3D-Druck"). Abgerufen von https://www.e-fi.de/fileadmin/Inhaltskapitel_2015/2015_B4.pdf

Gesellschaft für Datenschutz und Datensicherheit e.V. (2016). GDD-Praxishilfe DS-GVO III. To-Dos für die Übergangsfrist bis zur Geltung der DS-GVO. Abgerufen von https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_3.pdf

Gräßer, L. (2010). Datenschutz und Persönlichkeitsrechte im Web 2.0 – Kontrollverluste, „Einstellungssachen" und Entwicklungsherausforderungen. Abgerufen von http://www.grimme-institut.de/fileadmin/Grimme_Nutzer_Dateien/Institut/Dokumente/12_Datenschutz-Dossier_Grer.pdf

Hessen Trade & Invest GmbH (2015). Additive Fertigung. Der Weg zur individuellen Produktion. Abgerufen von http://www.haute-innovation.com/cms/upload/PDF/Additive_Fertigung_final_screen.pdf

Hessische Landesregierung. (2016). Strategie Digitales Hessen. Intelligent. Vernetzt. Für Alle. Abgerufen von https://www.digitalstrategie-hessen.de/img/Digitalstrategie_Hessen_2016_ver1.pdf

Isele, C., Kaufmann, P., Schütze, B., Spyra, G., Treinat, L., Wiedemann, M., & Wichterich, E. (2017). Leitfaden für die Erstellung eines IT-Sicherheitskonzeptes. Abgerufen von https://www.ztg-nrw.de/wp-content/uploads/2013/10/Leitfaden-f%C3%BCr-die-Erstellung-eines-IT-Sicherheitskonzeptes.pdf

ISO/ASTM (2015, Dezember). ISO/ASTM 52900:2015. Abgerufen 2. März, 2018 von https://www.iso.org/standard/69669.html

Kranig, T., & Ehmann, E. (2017). Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine: Das Sofortmaßnahmen-Paket. München: Bayerisches Landesamt für Datenschutzaufsicht. MIhaylov, Y.: Entstehungsgeschichte des Bundesdatenschutzgesetzes (BDSG), Präsentation http://users.minet.uni-jena.de/~nez/IuG200910/01.Entstehungsgeschichte%20des%20Bundesdatenschutzgesetzes.Mihaylov.pdf

Kühling, J., Martini, M., Heberlein, J., Kühl, B., Nink, D., Weinzierl, Q., & Wenzel, M. (2016). Die Datenschutz-Grundverordnung und das nationale Recht. Abgerufen von http://www.foev-spey-er.de/files/de/downloads/Kuehling_Marrtini_et_al_Die_DSGVO_und_das_nationale_Recht_2016.pdf

Lepperhoff, N., & Müthlein, T. (2017). Leitfaden zur Datenschutz-Grundverordnung. Zwickau: Datakontext.

Mihaylov, Y. (o.D.). Entstehungsgeschichte des Bundesdatenschutzgesetzes (BDSG). Abgerufen 6. März, 2018, von http://users.minet.uni-je-na.de/~nez/IuG200910/01.Entstehungsgeschichte%20des%20Bundesdatenschutzgesetzes.Mihaylov.pdf

Richter, S.; Wischmann, S. (2016). Additive Fertigungsmethoden – Entwicklungsstand, Marktperspektiven für den industriellen Einsatz und IKT-spezifische Herausforderungen bei Forschung und Entwicklung (Eine Studie im Rahmen der Begleitforschung des Technologieprogramms AUTONOMIK für Industrie 4.0 des Bundesministeriums für Wirtschaft und Energie). Abgerufen von https://vdivde-it.de/sites/default/files/document/Additive-Fertigungsmethoden-2016.pdf

Roland Berger (2016). Additive Manufacturing - next generation AMnx. Abgerufen von https://www.roland-berger.com/de/press/Neue-Studie-Rasanter-Fortschritt-bei-3D-Druck-Systemen.html

Schmidt, J., & Weichert, T. (Hrsg.). (2012). Datenschutz Grundlagen, Entwicklungen und Kontroversen. Bonn: Bundeszentrale für politische Bildung. Abgerufen von http://www.bpb.de/shop/buecher/schriftenreihe/143502/datenschutz

Schwartz, M., & Muhle, A. (2016). Chancen der Digitalisierung nutzen: Datenschutz und IT-Sicherheit gehören dazu (Nr. 117). Abgerufen von https://www.kfw.de/PDF/Download-Center/Konzernthemen/Research/PDF-Dokumente-Fokus-Volkswirtschaft/Fokus-Nr.-117-Februar-2016-Chancen-der-Digitalisierung-nutzen.pdf

Schwartz Public Relations. (2017). Zweiter jährlicher Bericht über den Stand von Ransomware. Abgerufen von http://www.schwartzpr.de/de/newsroom/Malwarebytes/Osterman%202017/Osterman_Studie_zu_Ransomware_in_deutschen_KMU.pdf

sculpteo (2017). The state of 3D printing. Abgerufen von https://www.sculpteo.com/media/ebook/State%20of%203DP%202017_1.pdf

Unabhängige Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK). (2017). Kurzpapier Nr. 1 Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO. Abgeru-fen von https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_K

Verein Deutscher Ingenieure. (2014). Statusreport Additive Fertigungsverfahren. Abgerufen von https://www.vdi.de/fileadmin/vdi_de/redakteur_dateien/gpl_dateien/VDI_Statusreport_AM_2014_WEB.pdf

Webseiten

3Druck.com. (2011, 18. Januar). Teil 2: Übersicht der aktuellen 3D-Druckverfahren. Abgerufen 31. Januar, 2018, von https://3druck.com/grundkurs-3d-drucker/teil-2-uebersicht-der-aktuellen-3d-druckverfahren-462146/

ActiveMind.AG. (2017, 25. September). Muster: Datenschutzkonzept nach DSGVO. Abgerufen 15. Februar, 2018, von https://www.activemind.de/datenschutz/dokumente/datenschutzkonzept/

Anderl, R., & Arndt, A. (2014, 24. September). Additive Manufacturing oder generative Fertigungsverfahren – vom Prototypen zur Massenfertigung? Abgerufen 1. Februar, 2018, von https://www.hessen-nanotech.de/mm/mm001/3D_Additive_Manufacturing_Anderl_TUD.pdf

Arte. (o.D.). Datenschutz im digitalen Zeitalter [Video]. Abgerufen 6. März, 2018, von https://www.arte.tv/player/v3/index.php?json_url=http%3A%2F%2Fapi.arte.tv%2Fapi%2Fplayer%2Fv1%2Fconfig%2Fde%2F070443-006-A&lang=de_DE&config=arte_info&autostart=0&embed=0

Bentz, V. (2017, 9. Februar). Was ist der Unterschied zwischen Datenschutz und Datensicher-heit? Abgerufen 12. Januar, 2018, von https://www.brandmauer.de/blog/it-security/was-ist-der-unterschied-zwischen-datenschutz-und-datensicherheit

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. (o.D.). Technische und organisatorische Maßnahmen gem. Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g) und Auftragsverarbeiter (Art. 30 Abs. 2 lit. d). Abgerufen 1. März, 2018, von https://www.bvdnet.de/wp-content/uploads/2017/06/Muster_Verz_der_Verarbeitungst%C3%A4tigkeiten_TOMs.pdf

Bitkom. (2017, 19. September). Privacy Conference EU-Datenschutzgrundverordnung – Wie gut ist die deutsche Wirtschaft vorbereitet? Abgerufen 2. März, 2018, von https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/09-September/Privacy-Conference/Bitkom-Charts-PK-Privacy-Conference-19-09-2017-final.pdf

Brands Consulting. (2017, 24. März). Unterschiede zwischen Datenschutz und Datensicherheit – Wieso Datensicherheit nicht immer zum Datenschutz beiträgt? Abgerufen 12. Januar, 2018, von https://brands-consulting.eu/unterschiede-zwischen-datenschutz-und-datensicherheit-wieso-datensicherheit-nicht-immer-zum-datenschutz-beitraegt#Was_ist_unter_Datensicherheit_zu_verstehen

Bundesministerium für Bildung und Forschung (2015, 27. März). Bekanntmachung des Bundesministeriums für Bildung und Forschung von Richtlinien zur Förderung im Themenfeld „Additive Fertigung – Individualisierte Produkte, komplexe Massenprodukte, innovative Materia-lien (ProMat_3D)". Abgerufen 2. März, 2018, von https://www.bmbf.de/foerderungen/bekanntmachung-1037.html

Bundesministerium für Bildung und Forschung (2016, 15. März). Bekanntmachung Richtlinie zur Förderung transnationaler Forschungsprojekte innerhalb des ERA-NET „M-era.Net II" „Materialwissenschaft und Werkstofftechnologien" – Themenschwerpunkt: Materialien für die Addi-tive Fertigung – in den Rahmenprogrammen „Vom Material zur Innovation" und „Innovatio-nen für die Produktion, Dienstleistung und Arbeit von morgen". Abgerufen 2. März, 2018, von https://www.bmbf.de/foerderungen/bekanntmachung-1173.html

Bundesministerium für Wirtschaft und Energie. (2018, 18. Januar). Machnig: Wir unterstützen KMU, damit EU-Datenschutz-Grundverordnung auch in der Praxis ein Erfolg wird! Abgerufen 6. März, 2018, von http://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2018/20180118-wir-unterstuetzen-kmu-damit-eu-datenschutz-grundverordnung-auch-in-der-praxis-ein-erfolg-wird.html

Datenschutz.org. (o.D.). Datenschutz im Internetzeitalter: Privatsphäre & globale Vernetzung im Konflikt. Abgerufen 16. Januar, 2018, von https://www.datenschutz.org/

Die Landesbeauftragte für den Datenschutz Niedersachsen. (2010, Oktober). Schutzstufenkon-zept des LfD Niedersachsen. Abgerufen 1. März, 2018, von https://www.lfd.niedersachsen.de/technik_und_organisation/schutzstufen/schutzstufen-56140.html

Fidelis Cybersecurity. (o.D.). Cyberkriminalität 2017 in Zahlen und Fakten. Abgerufen 17. Januar, 2018, von http://blog.wiwo.de/look-at-it/files/2017/12/Cyberkriminalit%C3%A4t2017_IG.jpg

Hessen Trade & Invest GmbH. (2018, 15. März). Cast-Workshop Recht und IT-Sicherheit. Abgerufen 6. März, 2018, von https://www.technologieland-hessen.de/termine/29425

IHK München und Oberbayern. (o.D.). Datenschutz-Folgenabschätzung. Abgerufen 27. Februar, 2018, von https://www.ihk-muenchen.de/de/Service/Recht-und-Steuern/Datenschutz/Die-EU-Datenschutz-Grundverordnung/Datenschutz-Folgenabsch%C3%A4tzung/

Institut für Digitale Ethik (IDE) an der Hochschule der Medien Stuttgart. (2017). 10 ethische Leitlinien für die Digitalisierung von Unternehmen. Abgerufen 17. Januar, 2018, von http://www.digitale-ethik.de/digitalkompetenz/10-ethische-unternehmensleitlinien/

It-daily.net. (2014, 3. Juli). 12 Maßnahmen für die Datensicherheit. Abgerufen 8. Februar, 2018, von https://www.it-daily.net/it-sicherheit/datenschutz/9374-12-massnahmen-fuer-die-datensicherheit

Krämer, A. (2017, 10. April). Wohlers Report 2017 verzeichnet 17,4 Prozent Wachstum in der weltweiten 3D-Druck-Industrie. Abgerufen 6. März, 2018, von https://www.3d-grenzenlos.de/magazin/marktforschung/wohlers-report-2017-3d-druck-27253733/

Kramer, R. (2015, 23. September). Die Hintergründe der EU-Datenschutzgrundverordnung und die Bedeutung für die Datenschutzbeauftragten in Deutschland. Abgerufen 18. Januar, 2018, von https://www.computas.de/_downloads/07-Kramer.pdf

Maenz, F. (2017, 14. Dezember). DSGVO & KMU: Was gibt es zu wissen für Datenschutzbeauftragte? [Blogeintrag]. Abgerufen 6. März, 2018, von https://blogs.business.microsoft.com/de-de/2017/12/14/die-dsgvo-und-die-rolle-des-datenschutzbeauftragten-in-kmu-kleinunternehmen-und-mittelstand/

Prang, H. (2013, 10. April). 3D Druck in der Praxis – Von der Idee zum fertigen Objekt – Teil 2. Abgerufen 2. Februar, 2018, von https://entwickler.de/online/webmagazin/3d-druck-in-der-praxis-von-der-idee-zum-fertigen-objekt-teil-2-4772.html

Protected Shops. (o.D.). Die Technischen und organisatorischen Maßnahmen nach der Datenschutz-Grundverordnung – Was bedeutet eigentlich Stand der Technik? Abgerufen 27. Febru-ar, 2018, von https://www.protectedshops.de/infothek/whitepaper/dsgvo-technische-und-organisatorischen-massnahmen

Solmecke, C. (o.D.). Die EU-Datenschutzgrundverordnung – was ändert sich 2018? Abgerufen 6. März, 2018, von https://www.wbs-law.de/it-recht/datenschutzrecht/die-eu-datenschutzgrund-verordnung/

Statista. Geschätzter Umsatz mit 3D-Druck-Produkten in Deutschland und weltweit im Jahr 2016 (in Milliarden Euro). Abgerufen 2. März, 2018, von https://de.statista.com/statistik/daten/studie/581411/umfrage/umsatz-mit-3d-druck-in-deutschland-und-weltweit/

Unabhängige Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK). (2017). Auslegungshilfen zum neuen Datenschutzrecht, Kurzpapiere der Datenschutzkonferenz. Abgerufen 2. März 2018, von https://www.datenschutz.hessen.de/neuesdatenschutzrecht.htm

Voigtländer, D., & Schmischke, T. (o.D.). Datenschutz in der Praxis. Abgerufen 15. Februar, 2018, von https://www.dgq.de/regional/dateien/DGQ-Vortrag_-_Datenschutz_in_der_Praxis.pdf

IMPRESSUM

Effekte der Europäischen Datenschutzgrundverordnung auf Additive Manufacturing
Studie im Auftrag der Hessen Trade & Invest GmbH

Herausgeber
Hessisches Ministerium für Wirtschaft,
Energie, Verkehr und Landesentwicklung
Kaiser-Friedrich-Ring 75
65185 Wiesbaden
www.wirtschaft.hessen.de

Projektträger
Hessen Trade & Invest GmbH
Technologieland Hessen
Konradinerallee 9
D-65189 Wiesbaden
Telefon: +49 611 950 17-85
Fax: +49 611 950 17-8466
E-Mail: info@technologieland-hessen.de
www.technologieland-hessen.de

HESSEN TRADE & INVEST
Wirtschaftsförderer für Hessen

Redaktion
Sebastian Hummel, Hessisches Ministerium für Wirtschaft, Energie, Verkehr und Landesentwicklung

Nicole Holderbaum, Hessen Trade & Invest GmbH
Daniel Schreck, Hessen Trade & Invest GmbH

Verfasser
atene KOM GmbH | Agentur für Kommunikation, Organisation und Management
Ulrich Plate
www.atenekom.eu

Gestaltung
Piva & Piva, Heidelberger Str. 93, 64285 Darmstadt

Druck
A&M Service GmbH, Hinter dem Entenpfuhl 13/15, 65604 Elz

Klimaneutral Drucken
powered by ClimatePartner°

Bildnachweis
© iStock/matejmo (Titel); Fotolia.com: Max40547 (S. 16), xiaoliangge (S. 29); everythingposs/Depositphotos S. 46)

Stand
Oktober 2018

HESSEN Hessisches Ministerium für Wirtschaft, Energie Verkehr und Landesentwicklung

Projektträger:

HESSEN TRADE & INVEST

Wirtschaftsförderer für Hessen