CORE®

DAS ENDE DER KARENZ: DATENSCHUTZ NUTZEN

Perspektivwechsel – gesetzliche Anforderungen als strategische Chance

Autoren
Magdalena Buski
Marc-André Dymala
Dr. Waldemar Grudzien

Autorenteam
Christian Böhning
Johannes von Bonin
Nadine Hofmann

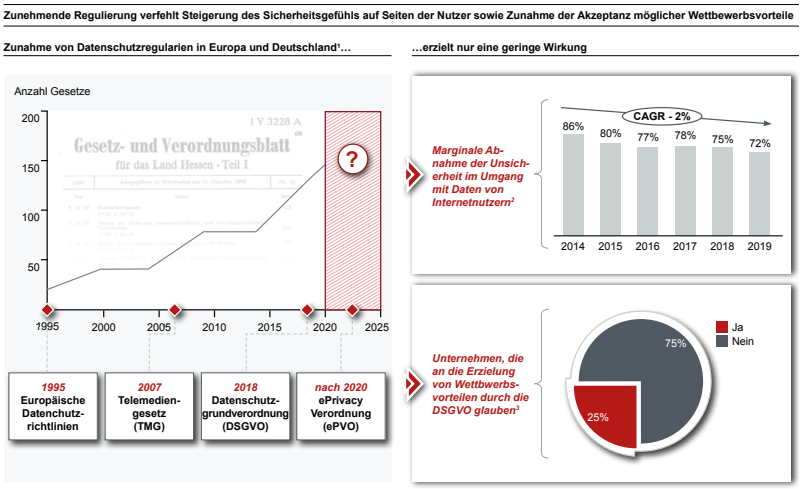
Juni 2020
White Paper

1 Einleitung

Daten und Vertrauen – Rohstoffe der Digitalwirtschaft

Was sind die Rohstoffe der digitalisierten Gesellschaft und damit wesentliche Produktionsfaktoren von künftig erfolgreichen Unternehmen? Sind es die Daten, welche regelmäßig als das neue Öl bezeichnet werden, oder ist vielmehr Vertrauen die entscheidende Ressource des 21. Jahrhunderts? Die Antwort ist: Beides – Daten und Vertrauen in die Verarbeitung dieser Daten. Vertrauen, dass die Daten konform mit dem Willen des Dateneigentümers und dem geschäftlichen Wert der Daten angemessen verarbeitet werden – beides mittlerweile reflektiert in gesetzlichen Regelungen, die einen Interessenausgleich zwischen den Teilnehmern der Digitalwirtschaft herstellen wollen. Schlüssel zur Erlangung dieses Vertrauens ist Datenschutz, kombiniert mit modernen Lösungen für die Informationssicherheit.

Regulatorische Vorgaben werden oft als Verhinderer von Innovationen, als Kostentreiber oder auch als notwendiges Übel wahrgenommen. Wir möchten mit dem vorliegenden Papier eine alternative Perspektive anbieten und zur Diskussion über Möglichkeiten des Datenschutzes als Wertbeitrag einladen. Unsere Überzeugung ist es, dass Datenschutz – richtig eingesetzt – Innovationstreiber sein kann und Chancenpotenziale bietet.



Quelle: COREresearch (2020) | 1 Der Europäische Datenschutzbeauftragte (2020), *Entwicklungsgeschichte der Datenschutz-Grundverordnung* | 2 Bitkom (2019), *Nutzervertrauen in Datensicherheit im Internet steigt* | 3 Der Informationsdienst des Instituts der deutschen Wirtschaft (2020), *Datenschutz: Ungeliebtes Regelwerk*

Abbildung 1: Wahrgenommene Wirkungsrichtung der Datenschutzgrundverordnung

Gesetzliche Regelungen für Datenschutz im Digitalen werden zunehmend durchgesetzt

Mit Inkrafttreten der EU-Datenschutzgrundverordnung (EU-DSGVO) bzw. General Data Protection Regulation (GDPR) im Mai 2016 und ihrer Anwendung seit Mai 2018 wurde ein umfassendes Regelwerk zum Schutz von persönlichen Daten geschaffen, welches seitdem in mehr als 100 Ländern weit über die EU hinaus adaptiert wird. So sehen wir sowohl in Kalifornien als Sitz der größten Global Player der Digitalisierung als auch z.B. in Indien die Einführung von Datenschutzgesetzen, die an die DSGVO angelehnt sind. Damit die DSGVO kein europäischer Exportschlager bleibt, den andere Regionen der Welt erfolgreich monetarisieren, müssen sich europäische Unternehmen gemäß ihrem Geschäftsmodell und ihren Ambitionen zu Datenschutz verhalten. Das vorliegende Papier bietet hierzu eine Handreichung. Kapitel 2 verdeutlicht die aktuelle Situation und zeigt auf, dass die Regelungen zunehmend in der Unternehmenswirklichkeit angekommen sind und die Aufsichtsbehörden diese auch konsequenter durchsetzen. Kennzeichen hierfür sind sowohl die Intensivierung der Überwachung als

auch die Verschärfung von Sanktionsmaßnahmen bei Verstößen gegen geltende Vorschriften. Umfragen zeigen, dass Unternehmen die Herausforderungen bzgl. Datenschutz ernst nehmen und umsetzen wollen, die Diskrepanz zwischen Anspruch und Realität allerdings noch hoch ist. Dies ist vor allem deshalb bedauerlich, weil die ohnehin vorhandenen Daten bei den Unternehmen einen immensen ökonomischen Nutzen darstellen, nur wird ihr Wertbeitrag aus Angst vor Datenschutzvergehen und einhergehenden Sanktionierungen nicht immer im eigentlichen möglichen Umfang genutzt. Einige wenige – nicht überraschend sind das gerade die globalen Technologiekonzerne – haben Datenschutz als Distinktionsmerkmal erkannt und richten ihre Produktfeatures gezielt danach aus.

Geschäftsmodelle ohne angemessene Berücksichtigung von Datenschutz nicht umsetzbar

Die dargestellte Situation reflektierend, betrachten wir in Kapitel 3 drei wesentliche Herausforderungen, denen sich Unternehmen bei Fragen des Datenschutzes und der Informationssicherheit ausgesetzt sehen:

- Gesetzliche Vorschriften zum Schutz persönlicher Daten sind zwingend und vollständig (im Sinne eines Mindestmaßes) umzusetzen, da jede Form von „Risikoakzeptanz“ aufgrund der Intensivierung der Überwachung und der Dimensionen möglicher (und bereits erfolgter) Sanktionen ausgeschlossen ist
- Viele bestehende Geschäftsmodelle basieren bereits heute auf der Verarbeitung von personenbezogenen Daten, die ohne Konformität zu den bestehenden und kommenden – Beispiel: ePrivacy-Verordnung – Datenschutzgesetzen unwirtschaftlich bzw. nicht mehr fortgesetzt werden können, sofern keine effizienten Lösungen zu finden sind
- Neue und innovative, auf Daten basierende Produkte und Services, werden entweder nicht am Markt angeboten oder sind verzögert, solange Datenschutzkonformität nicht effektiv und effizient gewährleistet werden kann. Damit verbundene wirtschaftliche Potenziale werden verschwendet und Marktpositionierungen unnötig gefährdet

In drei Stufen zum Datenschutz als integralen Strategiebestandteil

Um sowohl den Herausforderungen zu trotzen als auch die Chancen aus Datenschutz zu nutzen, stellen wir in Kapitel 4 ein Modell für den schrittweisen Aufbau von Datenschutz und -sicherheit vor. Das Modell beschreibt Ambitionsniveaus von einer Basisstufe zur Sicherstellung der gesetzlichen Mindestanforderungen, über einen souveränen Umgang mit erweiterten Datenschutzkonzepten zur aktiven Gestaltung von Vertrauensnetzwerken bis hin zur strategischen Positionierung von Datenschutz und Datensicherheit in der Gesamtstrategie als Treiber für Innovationen, Wachstum und Erschließung von Wettbewerbspotenzialen. Der gezielte Einsatz von IT zur effizienten Erreichung von Datenschutz ist inhärenter Bestandteil des Stufenmodells und wird ebenso erläutert wie Ausführungen zu erprobten Praxisbeispielen, bewährten Werkzeugen, Checklisten und geeigneten Vorgehensmodellen zum Aufbau von Datenschutz-Managementsystemen im Zusammenwirken mit Informationssicherheit.

Abschließend fassen wir unsere Empfehlungen zur proaktiven Gestaltung von Datenschutz, Daten- und Informationssicherheit zusammen. Diese Anregungen mögen somit dazu dienen, Vertrauen darin zu entwickeln, Datenschutz nicht nur als notwendiges Übel im Minimalprinzip umzusetzen, sondern die im Datenschutz liegenden Chancen und Potenziale im Maximalprinzip zu heben, um Vertrauen als wertvollste Ressource der Digitalwirtschaft aktiv zu erlangen und zu erhalten.

2 Einführung in die gegenwärtige Situation

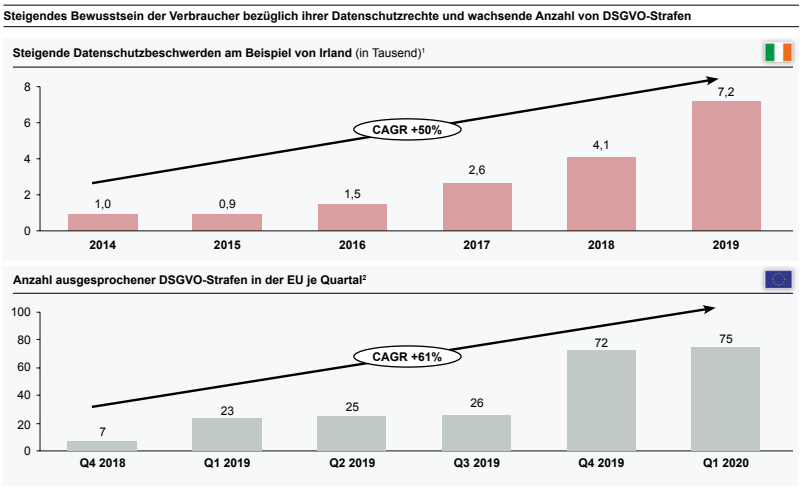
Datenschutz stellt für Unternehmen auch vier Jahre nach Verabschiedung der DSGVO eine Herausforderung dar. Immense Strafzahlungen verkörpern schwerwiegende Folgen von Datenschutzverletzungen. Trotz mittlerweile vierjähriger Gültigkeit, zweijähriger verbindlicher Anwendung, erster Sanktionsentscheide und zunehmend selbstbewusstem Vorgehen der Datenschutzaufsichtsbehörden liegt den meisten Unternehmen die DSGVO-Konformität noch immer fern. Dysfunktionale strategische und handwerkliche Umsetzung – gepaart mit einer Überschätzung der eigenen Datenschutzfähigkeiten – wirken in einem zunehmend datengetriebenen Markt als Herausforderung und erhöhen den Kosten- und Wettbewerbsdruck auf Unternehmen mit wachsender Tendenz.

2.1 Datenschutzverstöße mit sehr hohen Bußgeldern belegt

Internationale Verdichtung und Ausdifferenzierung von Datenschutzgesetzen für die digitale Welt

Verbraucher, insbesondere in Deutschland und Europa, haben in den letzten Jahren ein ausgeprägtes Bewusstsein für Datenschutz entwickelt. Diese Sensibilisierung gründet nicht zuletzt auf Datenschutzverletzungen, die Millionen Nutzer betrafen, wie etwa zahlreiche Vorfälle im Zusammenhang mit großen Technologieplattformen. Zugleich hat sich der Gesetzgeber sowohl auf deutscher als auch auf europäischer Ebene dem Thema Datenschutz verstärkt gewidmet. Das prominenteste Beispiel ist sicherlich die im Jahr 2016 in Kraft getretene DSGVO.

Das Bundesverfassungsgericht (BVerfG) leitet das Recht auf informationelle Selbstbestimmung aus dem allgemeinen Persönlichkeitsrecht nach Artikel 2 i.V.m. Artikel 1 Grundgesetz ab. Demnach wird die Hoheit über die eigenen Daten als Bestandteil der geschützten individuellen Entfaltung verstanden. Nach dieser Wertung soll der Einzelne gegen jede Form der Weitergabe und Verwendung personenbezogener Daten ohne sein Einverständnis geschützt werden. Mit der Stärkung der Datenschutzrechte und der Festigung des Rechtsbewusstseins der Verbraucher/ Betroffenen steigt auch die Anzahl der Beschwerden deutlich (Abbildung 2). Länder wie Irland, oftmals europäischer Sitz globaler Datenverwerter, zeigen, welche Folgen das für Datenschutz sensibilisierte Bewusstsein, aber auch die Verpflichtung zur Selbstanzeige nach Artikel 33 DSGVO haben kann.



Quelle: COREresearch (2020) | 1 Irish Data Protection Commission (2020), *Annual Report 2019* | 2 CMS (2020), *GDPR Enforcement Tracker*

Abbildung 2: Anstieg von datenschutzrechtlichen Beschwerden und Strafen

Europaweit ist ein deutlicher Anstieg der ausgesprochenen Bußgelder seit der Einführung der DSGVO zu beobachten. Steigende Anforderungen von Regulator, Aufsicht und Kunden in Bezug auf Datenschutz erhöhen den Druck auf europäische Unternehmen. Seit der Einführung der DSGVO werden weltweit Datenschutzregularien verstärkt. Länder wie die USA, China, Japan und Argentinien ziehen nach.[1] Kalifornien, siebtgrößte Wirtschaftsregion der Welt, orientiert sich mit dem *California Consumer Privacy Act (CCPA)* stark an dem europäischen Gesetz.

Während der CCPA jedoch erst dieses Jahr in Kraft getreten ist und damit Unternehmen bislang von den Folgen von Datenschutzverletzungen verschont blieben[2], ist die „Schonfrist" für europäische Unternehmen vorbei. Denn bereits im letzten Jahr ließ sich ein zunehmend durchsetzungsstarkes Vorgehen der Datenschutzaufsichtsbehörden beobachten: 2018 lag die durchschnittliche Höhe der Bußgelder pro Monat bei EUR 48.000, im Jahr 2019 entsprach die durchschnittliche Bußgeldhöhe pro Monat hingegen bereits EUR 2,9 Mio., was einen Anstieg von 5.936 % im ersten Jahr verkörpert – offene Fälle ausgenommen.[3]

Deutlicher Anstieg der Höhe der Bußgelder im 2. Jahr der Anwendung der DSGVO (Mai 2018)

Zu den wohl bekanntesten Beispielen hoher Bußgelder aufgrund von Datenschutzverletzungen zählt das Unternehmen British Airways.

Gesetzgeber schöpft Strafmaß der DSGVO in mehreren Fällen aus (exemplarisch)

Unternehmen	Land	Datum	Verstoß DSGVO	Details zum Gesetzesverstoß	Strafe in EUR Mio.
British Airways		08.07.2019	Art. 32	Umleitung des Benutzerverkehrs auf der Webseite auf eine betrügerische Seite	213
Marriott		09.07.2019	Art. 32	Data Breach: Offenlegung personenbezogener Daten von 339 Mio. Datensätzen	110
Google		21.01.2019	Art. 4, 5, 6,11, 13 und 14	Einrichtung Google-Konto bei Konfiguration eines Mobiltelefons mit Android	50
TIM		15.01.2020	Art. 5, 6, 17, 21 und 32	Werbung trotz Widerspruch; unrichtige Information über Datenverarbeitung, Löschfristen	28
Österr. Post AG		23.10.2019	Art. 5 (1), 6	Unerlaubtes Sammeln und Weiterverkaufen von Parteiaffinität bei 2,2 Mio. Betroffenen	18
Deutsche Wohnen		30.10.2019	Art. 5, 25	Archivierung ohne Löschfunktion, Speicherung ohne Prüfung von Notwendigkeit/ Zulässigkeit	15

Quelle: CMS (2020), *GDPR Enforcement Tracker*

Abbildung 3: Auswahl ausgesprochener Bußgelder nach DSGVO

Der Begriff „British Airways Datenschutzskandal" ergibt über eine Million Suchergebnisse bei Google, was durchaus als Indikator für ein gestiegenes Bewusstsein der Verbraucher bzgl. ihrer Datenschutzrechte gewertet werden kann. Der hiermit verbundene Reputationsschaden für das Unternehmen ist immens und verursacht vermutlich ebenso hohe Kosten, wie das direkt verhängte Bußgeld in Höhe von EUR 213 Mio. Das Beispiel verdeutlicht, welche wirtschaftlichen Folgen Unwissenheit, Untätigkeit oder gar Missachtung des Themas Datenschutz haben können.

Datenschutzverletzungen haben hohe direkte und indirekte monetäre Folgen für Unternehmen

[1] Accessnow (2019), S.36.

[2] Ausbleibende Bußgelder beziehen sich auf in den USA ausgesprochene Bußgelder. Amerikanische Unternehmen, die mit europäischen personenbezogenen Daten oder in Europa agieren, fallen in Europa unter die DSGVO.

[3] CMS (2020), 24.04.2020.

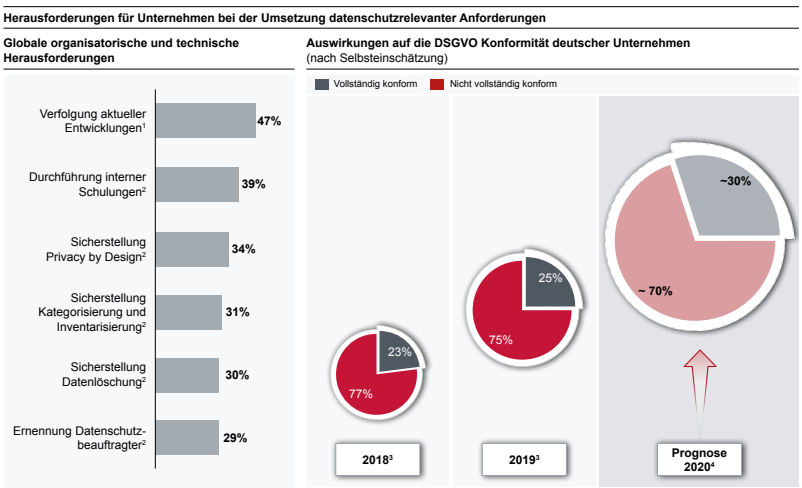
Datenschutzaufsichtsbehörden scheuen europaweit nicht davor zurück, hohe Bußgelder zu verhängen. Dabei kann die Bußgeldhöhe entweder in den gesetzlichen Regelungen definierte EUR 20 Mio. oder bis zu 4 % des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs betragen.

2.2 Diskrepanz zwischen Selbsteinschätzung und Datenschutzkonformität: 70 % der Wirtschaft schlecht vorbereitet

Über 40 % der Unternehmen weltweit sind mit der Umsetzung von Datenschutzanforderungen überfordert

Die oben beschriebenen Begebenheiten sollten vielen Unternehmen als Warnung gelten. Analysen und aktuelle Projekterfahrungen zeigen, dass die meisten Unternehmen auch vier Jahre nach Verabschiedung der DSGVO nicht datenschutzkonform agieren. Auch Unternehmen, die sich selbst als konform einschätzen, sind es in Wirklichkeit aufgrund handwerklicher Fehler oftmals nicht. Die Umsetzung der DSGVO-Anforderungen stellt viele Unternehmen vor Herausforderungen. International geben 42 % der Unternehmen an, Schwierigkeiten bei der Erfüllung von Anforderungen an die Datensicherheit, d.h. an die von der DSGVO geforderten technischen und organisatorischen Maßnahmen (TOM), zu haben.

Organisatorische Herausforderungen spiegeln sich in einer Unsicherheit im Umgang mit Datenschutz im Unternehmen wider. Diese Unsicherheit entsteht durch einen Mangel an geeigneten Fachkräften und fehlenden Schulungen sowie zu geringem Budget im Bereich Datenschutz. Ebenso stellt die sich kontinuierlich weiterentwickelnde Regulatorik und der aktuell noch relativ hohe Interpretationsspielraum bei der Auslegung von Datenschutzgesetzen ein Problem dar. So haben laut Umfragen 47 % der Unternehmen weltweit Schwierigkeiten, den Überblick über Datenschutzregularien zu behalten oder befürchten, in Ihrem bereits niedrigen Wissensstand weiter zurückzufallen.



Quelle: COREresearch (2020) | 1 Thomson Reuters (2019) Survey, *GDPR+1 YEAR*; TrustArc (2018), *GDPR Compliance Status* | 2 Cisco (2019), *Data Privacy Benchmark Study* | 3 Bitkom (2019) *DSGVO, ePrivacy,* Brexit - Datenschutz *und die Wirtschaft* | 4 Expertenschätzung COREresearch

Abbildung 4: Schwierigkeiten bei der praktischen Umsetzung der DSGVO

Einen deutlich größeren Einfluss auf die Überforderung bei der Umsetzung von Datenschutzanforderungen haben notwendige technische Maßnahmen. 34 % der Unternehmen haben erhebliche Schwierigkeiten, den gesetzlich manifestierten „Datenschutz durch Technikgestaltung“ (Privacy-by-Design) zu erfüllen. Auch die Gewährleistung des „Rechts auf Vergessenwerden“, also das Löschen personenbezogener Daten, stellt für 30 %

der Unternehmen eine Herausforderung dar. Bei einer Vielzahl (36 %)[4] von Unternehmen fehlt grundsätzlich ein Verständnis für die toolgestützte Umsetzung der DSGVO-Anforderungen, welches auch mittels organisatorischer Maßnahmen nicht ausgeglichen werden kann. Die Überforderung mündet in einer letztlich geringen Anzahl an DSGVO-konformen Unternehmen: In Deutschland liegt ihr Anteil nach Selbsteinschätzung bei rund einem Viertel in 2019; vermutlich ca. einem Drittel in 2020.

2019 schätzten sich nur 25 % der deutschen Unternehmen als vollständig konform mit Datenschutzgesetzen ein

Wie so oft, steht die Realität jedoch mit der Eigenwahrnehmung in Diskrepanz. Unsere Projekterfahrung hat gezeigt, dass selbst Unternehmen, die davon ausgehen, vollständig DSGVO-konform zu agieren, wichtige Aspekte übersehen:

- Gesetzliche Mindestanforderungen an den Datenschutz wie ein Verarbeitungsverzeichnis, Löschkonzept oder eine TOM-Dokumentation sind entweder nicht vorhanden oder in einem Zustand niedriger Qualität
- Datenschutzbeauftragte werden zwar benannt, jedoch der Datenschutzaufsicht nicht immer wie vorgeschrieben gemeldet
- Interne Audits zur Umsetzung von datenschutzbezogenen Regularien finden nicht statt
- Die Umsetzung der Betroffenenrechte fehlt vollständig oder ist als mangelhaft einzuschätzen
- Cookie-Management in öffentlichen Web- und Mobile-Angeboten wird nicht gesetzeskonform umgesetzt
- Eine konforme Löschung von Daten, nach Fristablauf oder auf Anforderung, wird nicht gewährleistet

Wiederkehrende Hauptursache der auftretenden Aspekte ist eine fehlende technische Unterstützung und kein adäquater Umgang mit IT-Lösungen, um Datenschutz und Datensicherheit in digitalen Prozessen zu gewährleisten.

2.3 Wachstum der Datenmenge beinhaltet großes ökonomisches Potenzial

Daten sind zunehmend digital verfügbar und die Menge der verarbeiteten Daten steigt. Laut Prognose wird die weltweite Menge der Daten bis 2025 jährlich und über alle Branchen hinweg um 27 % anwachsen. Nicht alle diese Daten sind personenbezogene Daten im Sinne der Datenschutzgesetze wie der DSGVO, aber viele sind personenbeziehbar oder entfalten besonderen ökonomischen Wert in der Anwendung gegenüber Nutzern, Verbrauchern, Mitarbeitern, Geschäftspartnern und Kunden.

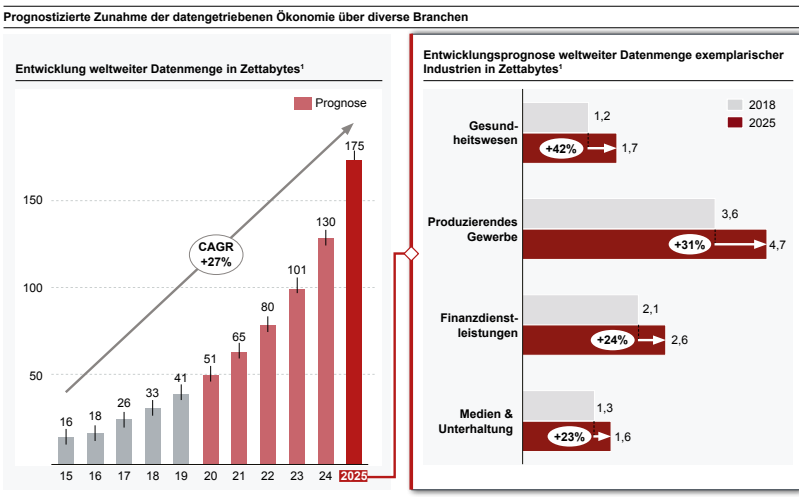
Digitale Verfügbarkeit und Verarbeitung von Daten steigt fortlaufend an

Selbst ehemals „analoge“ Branchen, wie beispielsweise das produzierende Gewerbe oder das Gesundheitswesen, können einen Anstieg an digitalen personenbezogenen Daten erwarten. Folglich sind materielle Endprodukte und manuelle Arbeitsvorgänge keine Schutzgarantie vor der Digitalisierung. Bis 2025 werden im Gesundheitswesen 36 %, im produzierenden Gewerbe 30 % mehr Daten prognostiziert. Zum weiteren Anstieg der Datenmenge trägt das „Internet (of Things)“ bei. Anwendungen wie Smart Home, Smart City bis hin zu Smart Health verschieben das Wirtschaftsgeschehen vermehrt ins Internet. Dies geschieht freiwillig aus eigener strategischer Entscheidung, oder wird durch GAFAM[5] und BATX[6] de facto erzwungen. Als Rückkopplung führt diese Entwicklung zu einem weiteren Anstieg der Daten – das „Daten Perpetuum Mobile“ ist erschaffen.

[4] TrustArc (2018), S. 10.

[5] Google, Apple, Facebook, Amazon, Microsoft.

[6] Baidu, Alibaba, Tencent, Xiaomi.



Quelle: COREresearch (2020) | 1 Der Informationsdienst des Instituts der deutschen Wirtschaft (2019), *Datenmenge explodiert;* IDC (2018): *The Digitization of the World*

Abbildung 5: Entwicklung der Gesamtdatenmenge je Branche und weltweit

Steigende Datenmengen beinhalten Geschäftspotenzial, wenn Datenschutz effizient realisiert ist

Die mengenbegründete Potenzialerschließung digitaler Daten, vielversprechende Möglichkeiten der Datenverwertung durch neue Techniken wie Künstliche Intelligenz (KI) sowie die Erschließung neuer Geschäftsfelder sind die eine Seite der „Datenmedaille“. Eine Zunahme von Daten ist zumeist gleichbedeutend mit einer Zunahme von personenbezogenen Daten. Diese Entwicklung konfrontiert Unternehmen, die datenschutzrelevante Vorgänge manuell ausführen, mit einer Kostenexplosion, weil Kosten- und Zeitaufwände manueller Verarbeitung potenziell mit steigender Datenmenge wachsen. Da dieser Umstand, wie im vorherigen Kapitel beschrieben, die meisten Unternehmen betrifft, steht die generierte Datenflut oft mit der Wahrung von Datenschutz im Konflikt. Grundsätze der DSGVO, wie Datenminimierung oder Speicherbegrenzung im Sinne des Artikel 5 Abs. 1 c), e) DSGVO können nur schwer gewährleistet werden.

Neben selbst verursachten Fehlern kann die Datenmaximierung ebenso zu indirekt verursachten Fehlern bei der Verarbeitung durch Dritte führen. Beispielsweise schafft die Menge an produzierten und genutzten Daten die Notwendigkeit von hohen Speicherkapazitäten, die Unternehmen wirtschaftlich sinnvoll nicht allein bereitstellen können. Ausgelagerte Backups, Archive, aber auch die Vernichtung von Datenträgern gehören schon lange zu den typischen Auftragsverarbeitungstätigkeiten. Nun werden diese zusätzlich um internet- oder cloudbasierte Speichermöglichkeiten von Drittanbietern ergänzt. Diese Auftragsverarbeiter können z.B. Data Warehouse Dienste sein, die Big Data Analysen ermöglichen. Ergänzend verarbeiten multiple, in Clouds betriebene Tool-Umgebungen personenbezogene Daten in Entwickler-, Marketing- und Analyse-Tools und geben diese an Auftragsverarbeiter weiter. Dem Auftragsverarbeitungsgeber ist ggf. gänzlich unbekannt, welches Tool die Daten seiner Kunden ohne deren Erlaubnis verarbeitet.

Problematisch ist dabei, dass die Daten zwar in den Machtbereich dieser Drittanbieter gelangen, der Verantwortliche jedoch verantwortlich bleibt. Der Auftragsverarbeiter handelt im Namen des Verantwortlichen, dieser hat gemäß Artikel 28 Abs. 1 sowie Erwägungsgrund 81 der DSGVO sicherzustellen, dass der Auftragsverarbeiter „Fachwissen, Zuverlässigkeit und Ressourcen, hinreichende Garantien dafür bietet, dass technische und organisatorische Maßnahmen – auch für die Sicherheit der Verarbeitung getroffen werden“. Bei einer fehlerhaften Datenverarbeitung seitens des Auftragsverarbeiters haftet der Verantwortliche gemäß Artikel 82 Abs. 4 DSGVO gesamtschuldnerisch mit den Auftragsverarbeitern für das Vergehen.

Datenverarbeitung wird vermehrt ausgelagert – Unternehmen haften für Fehler externer Dritter

Vergehen von Auftragsverarbeitern haben neben der Haftung zusätzliche reputationsrelevante Auswirkungen für den Verantwortichen. Nicht der Auftragsverarbeiter, sondern der Verantwortliche hat Datenschutzverletzungen, die voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiteiten haben, bekanntzumachen. Er muss sowohl die Datenschutzaufsicht gemäß Artikel 33 DSGVO, als auch die betroffenen Personen gemäß Artikel 34 benachrichtigen.

So verstärkt die Generierung von immer neuen Daten die Überforderung der Unternehmen bei der Umsetzung von Datenschutzanforderungen. Risiken und Folgen der internen aber ebenso externen Datenverarbeitung sind mit einer Datenschutz-Folgenabschätzung (DSFA) zu bewerten und mit adäquaten technisch-organisatorischen Maßnahmen zu behandeln. Hierfür müssen Datenflüsse und Datenquellen bekannt sein und die Expertise zur technischen und fachlichen Umsetzung von Datenschutz existieren. Diese Voraussetzungen können Unternehmen oft nicht gewährleisten. Was einen möglichen Erklärungsansatz dafür bietet, wieso notwendige Investitionen in Datenschutz nicht (ausreichend) getätigt werden oder bislang ein Risiko von Bußgeldern für Datenschutzverletzungen durch fehlende Konformität aufgrund von zu hohen manuellen Umsetzungskosten in Kauf genommen wird.

Grundsätzlich positive Datengenerierung wirkt verstärkend auf die Überforderung bei Wahrung von Datenschutz

3 Erfolgreiche Geschäftstätigkeit ist ohne Datenschutz nahezu unmöglich

Aufsichtsbehörden üben zunehmend Druck auf Unternehmen aus. Sie greifen strenger durch, weiten Kontrollen und Bußgelder auf immer mehr Branchen und Unternehmen aus. Gleichzeitig sind bereits neue regulatorische Datenschutzanforderungen im Gesetzgebungsverfahren, denn die ePrivacy-Verordnung (ePVO) wird den regulatorischen Druck zusätzlich erhöhen. Als Folge der gesetzlichen Fortentwicklung wird die Evolution der Unternehmen gehemmt. Nicht aber etwa durch die Regelungen selbst, sondern aufgrund von strategischer Fehlbewertung des Wertes von Datenschutz und Angst vor Datenschutzvergehen durch die Unternehmen.

3.1 Risikoakzeptanz ist keine Option mehr

Aufsichtsregime wird verdichtet – Aufsichtsbehörden schöpfen volles Strafmaß zunehmend aus

Während zunächst etablierte Unternehmen mit hohen Bußgeldern belegt wurden, stehen nun vermehrt auch kleinere Unternehmen bis hin zu Privatpersonen im Fokus der Datenschutzaufsichtsbehörden.

Insgesamt wurden seit der Einführung der DSGVO in Deutschland Bußgelder mit einem Volumen von insgesamt ca. EUR 25 Mio. verhängt. Mittlerweile umfasst die durchschnittliche Summe je Datenschutzvergehen ca. EUR 1 Mio. im Vergleich zu rund EUR 9.100 im Jahr 2018.[7] Die Aufsicht nutzt über sämtliche Branchen hinweg ihr Aufsichtsregime vollends aus:

Exemplarische Bußgelder nach DSGVO-Verstößen in Deutschland (je Branche)

Branche	Betroffene	Beschreibung des Verstoßes	Bußgeld in TEUR
Immobilien	Deutsche Wohnen SE	Nicht konforme Archivierung (Art. 25 DSGVO)	14.500
Tele-kommunikation	1&1 Telecom GmbH	Unrechtsgemäße Weitergabe personenbezogener Daten/ unzureichende technische und organisatorische Maßnahmen (Verstoß geg. Art. 32 DSGVO)	9.550
Lieferdienste	Delivery Hero Germany GmbH	Speicherung ohne Rechtsgrundlage/ Missachtung des Rechts auf Löschung (Art. 15/ 17/ 21 DSGVO)	195
Gesundheits-wesen	Krankenhaus in Rheinland-Pfalz	Veröffentlichung von Gesundheitsdaten/ unzureichende technische und organisatorische Maßnahmen (Art. 32 DSGVO)	80
Finanzindustrie	N26	Speicherung ohne Zustimmung der Betroffenen (Art. 6 DSGVO)	50
Verkehrsdienste	Hamburger Verkehrsverbund GmbH	Nicht-Meldung von Sicherheitslücken der Website trotz Aufmerksammachung durch Kunden (Art. 33/ 34 DSGVO)	20
Soziale Netz-werke	Knuddels.de	Enthüllung von personenbezogenen Daten durch Hackerangriff (Art. 32 DSGVO)	20
Gastronomie	Restaurant im Saarland	Unrechtmäßige Videoüberwachung von Kunden (Art. 5 DSGVO)	2
Öffentlicher Dienst	Beamter – Polizei	Rechtswidrig dienstlich erlangte personenbezogene Daten (Art. 6 DSGVO)	1,4
Privatpersonen	Bürger	Veröffentlichung von Aufnahmen des öffentlichen Straßenverkehrs auf YouTube, ohne Einwilligung der Betroffenen (Art. 5 DSGVO)	0,2

Quelle: CMS (2020), *GDPR Enforcement Tracker*

Abbildung 6: Exemplarische Bußgelder nach Artikel 83 DSGVO in Deutschland 2018–2019

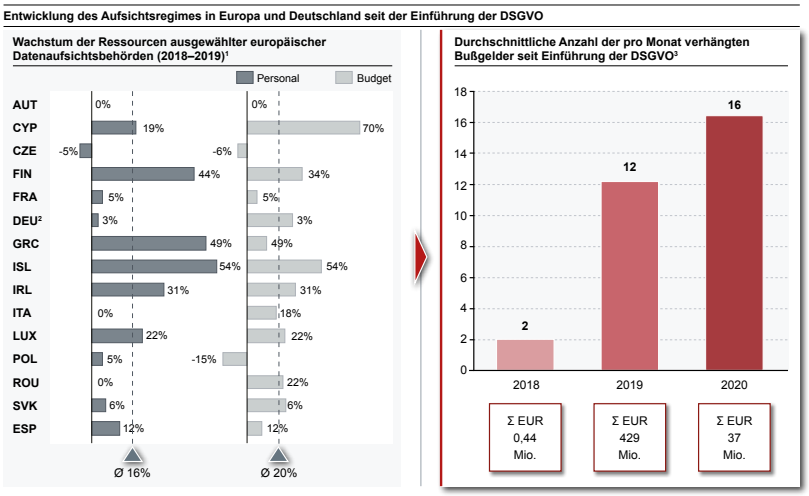
Verstecken im Schatten der Großen ist vorbei – breite Wirtschaft im Fokus

Bereits Ende letzten Jahres richtete sich der Fokus von datenschutzrelevanten Sanktionen zusehends auch auf kleine Unternehmen und kleinere Verstöße. Beispielsweise wurde einem Polizeibeamten ein Bußgeld in Höhe von EUR 1.400 wegen rechtswidrig dienstlich erlangter personenbezogener Daten auferlegt (Abbildung 6).

[7] CMS (2020), 03.05.2020.

Aufsichtsbehörden rüsten personell und finanziell überproportional auf

Die zunehmende Entwicklung der Bußgelder in Anzahl und Höhe spricht für sich. Zukünftig werden immer mehr Unternehmen mit Kontrollen der Aufsicht rechnen und mit den Folgen einer Prüfung leben müssen. Eine Vermutung, die durch zwei zusätzliche Kenngrößen bestätigt wird: Die monatliche Anzahl ausgesprochener Bußgelder steigt überproportional. Zusätzlich wurden europaweit bereits 2019 personelle (bis zu 30 % Anstieg zum Vorjahr) und budgetäre Ressourcen (bis zu 70 % Anstieg zum Vorjahr) bei Datenschutzbehörden aufgestockt. In Deutschland kam es 2019 zu einem Budgetanstieg von 28 % und zu einer Aufstockung an personellen Ressourcen um 3 %, wobei sich diese Ergebnisse aus Angaben von nur 7 deutschen Landesbehörden und der Bundesbehörde zusammensetzten, die Autoren gehen von einem vergleichbaren Vorgehen in den weiteren Bundesländern aus. Im Jahr 2020 soll sich der personelle Anstieg zusätzlich erhöhen, denn der Bundestag kündigte die Schaffung von 27 % zusätzlicher Stellen bei Datenschutzaufsichtsbehörden bis Ende 2020 an.[8] Folglich wird Risikoakzeptanz in Zukunft keine Option mehr darstellen, denn kein Unternehmen kann sich mehr „im Schatten der Großen“ vor der Aufsicht verstecken.



Quelle: 1 European Data Protection Board (2019), *Report on the implementation of GDPR* | Anmerkungen: 2 Basierend auf Informationen, die von der Bundes- und 7 Landesbehörden zur Verfügung gestellt wurden | 3 CMS (2020), *GDPR Enforcement Tracker*

Abbildung 7: Entwicklung des Aufsichtsregimes und durchschnittlichen Anzahl pro Monat verhängter DSGVO-Bußgelder

Datenschutzvorfälle resultieren oft aus Vorfällen der Informationssicherheit

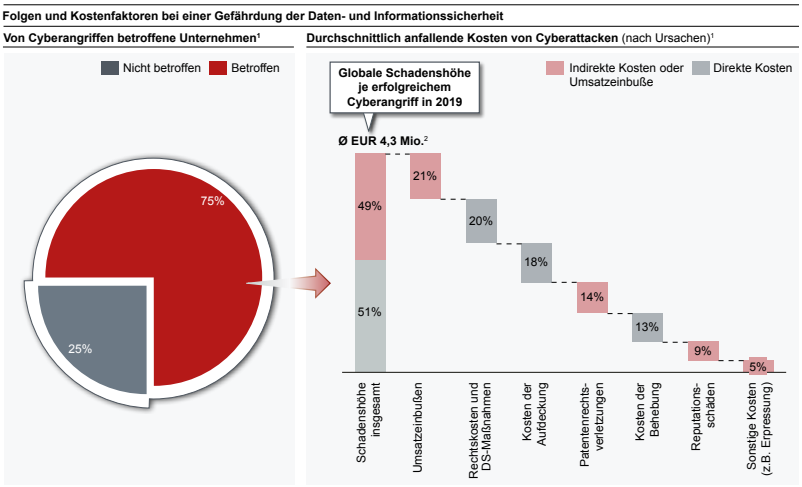
Der Blick zur Aufsicht ist zwar ein sehr wichtiger, aber nicht die einzige notwendige Betrachtungsweise. Die bereits hohen datenschutzrechtlichen Kosten sind nämlich eine bloße Teilmenge der Gesamtkosten einer Datenschutzverletzung. Exemplarisch lassen sich die durchschnittlichen Gesamtkosten von EUR 4,32 Mio. je Vorfall mit Verletzung der Datensicherheit darstellen. Datenpannen und Cyberattacken legen zumeist Kreditkartendaten, Daten von App-Nutzern, Passwörter und persönliche Daten inkl. Fotos[9] offen, was sie zu datenschutzrechtlichen Vorfällen macht. Allein im Jahr 2019 waren 75 % der deutschen Unternehmen von Cyberattacken betroffen. Vorfälle, die bei nicht ausreichenden technischen und organisatorischen Maßnahmen im Sinne von Artikel 32 DSGVO mit hohen Bußgeldern geahndet werden. Dennoch nehmen Sanktionskosten letztlich nur ca. 20 % der Gesamtkosten ein.

[8] Heise online (2019), 15.05.2020.

[9] Handelsblatt (2019), S.16.

Die Gesamtkosten setzen sich aus mehreren direkten und indirekten Komponenten zusammen. Direkte Kosten entstehen durch Aufwände der Aufdeckung: Unternehmen benötigen durchschnittlich 69 Tage[10], um Datenlecks zu finden und zu beheben – 69 Tage mit Behinderung des Betriebsablaufs, da Systeme zunächst offline gehen müssen – 69 Tage in denen automatisierte Vorgänge manuell ausgeführt werden müssen, in denen somit die Produktivität deutlich abnimmt und Erlöse gemindert werden oder gar ausfallen – 69 Tage die 18 % der Gesamtkosten von Datenlecks verursachen. Im Bereich indirekter Kosten verursachen Reputationsschäden mit immerhin 9 % einen weiteren datenschutzrelevanten Kostenblock von Cyberattacken.

30 % der Gesamtkosten einer Gefährdung der Datenschicherheit entfallen auf Umsatzeinbußen (21 %) und Reputationsschäden (9 %), die darüber hinaus zusätzlich nachwirken



Quelle: 1 Bitkom (2019), *Angriffsziel deutsche Wirtschaft: mehr als 100 Milliarden Euro Schaden pro Jahr;* Prozentzahlen wurden aus Ursachen der Cyberangriffskosten der letzten zwei Jahre abgeleitet | 2 Geldinstitute (2020), *Millionenschäden: Die Kosten eines Datenlecks*

Abbildung 8: Kostenanteile von Sicherheitsvorfällen im Datenschutz

So verursachte Reputationsschäden entfalten ihre Wirkung noch lange nach dem tatsächlichen Vorfall, denn Nutzer werden zunehmend sensitiv und durch mediale Vernetzung erreichen negative Schlagzeilen einen weiten Adressatenkreis, wodurch sowohl bei Bestandskunden, als auch bei Neukunden Datenschutzbedenken hervorgerufen werden.

3.1 Bestehende Geschäftsmodelle geraten unter Druck – Anpassungsbedarf an Datenschutzgesetze

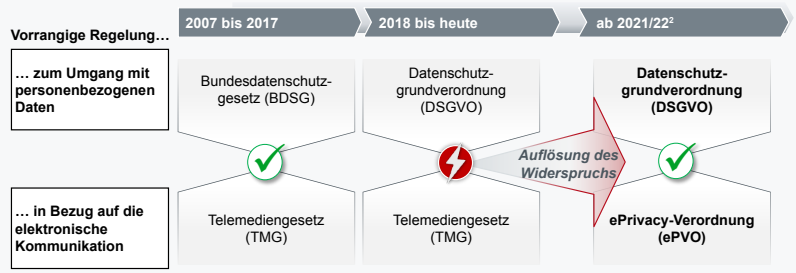
Im datengetriebenen Markt sind Cookies, Tracking, Consent und Profiling bekannte Schlagwörter, die bei Unternehmen im Rahmen ihres Marketings bereits vielfache Anwendung finden. Gleichzeitig sind es auch Schlagwörter, die stark im Fokus der Diskussion um Datenschutz zwischen Regulator, Aufsichten, Verbraucherschutzorganisationen und der Wirtschaft stehen, denn die rechtliche Ausgestaltung ihrer Verwendung im Online Marketing ist ungeklärt. Kern der Diskussion ist die Frage, auf welcher Rechtsgrundlage Daten der Nutzer (Nutzerdaten und Nutzungsdaten) durch First Party genutzt und an Third Party (Werbenetzwerke, Google, Facebook etc.) weitergeleitet werden dürfen. Bedarf es für die beabsichtigte Verarbeitung der personenbezogenen Daten für Tracking, Werbung und Bildung von Nutzerprofilen – zusammengefasst zu „Datendienste“ – eines Einverständnisses des Nutzers?

Rechtlicher Umgang mit Cookies, Tracking, Consent und Profiling ungewiss – Abhilfe sollen ePVO und TMG Novelle schaffen

[10] Die Welt (2018), 18.05.2020.

Eine Frage bei der Wirtschaftssubjekte bisher keine Einigung erlangen konnten: Die Datenschutzaufsicht verlangt eine Einwilligung nach Artikel 6 Abs. 1 a DSGVO. Die Online-Werbeindustrie wie zum Beispiel Medienhäuser verweisen auf § 15 Abs. 3 TMG (Telemediengesetz), wonach die bedarfsgerechte Gestaltung von Telemedien die Nutzung pseudonymer Nutzungsprofile mit Widerspruch (Opt-Out) erlaube bzw. nach Artikel 6 Abs. 1 f DSGVO das berechtigte Interesse des Medienhauses als höherwertig einzustufen sei als das berechtigte Interesse des Nutzers, seine Daten nicht für Datendienste zu nutzen. Diese Unklarheit führt zu weiterhin bestehendem Interpretationsspielraum bei der Auslegung der Rechtsprechung, die z. B. Webseitenbetreiber zur Steigerung der Konversionsrate beim pseudonymen Nutzertracking aktiv ausnutzen. Abhilfe bei dieser Diskussion und Präzisierung der DSGVO im Bereich der elektronischen Kommunikation soll die ePVO und die TMG-Novelle schaffen:

Unterschiedliche Zielrichtungen von DSGVO und TMG – ePVO das „Zünglein an der Waage“[1]



Quelle: COREresearch (2020) | 1 Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) *in der aktuellen Version des ABl. L 119, 04.05.2016* | Bundesministerium der Justiz und für Verbraucherschutz (2007), *Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 11 des Gesetzes vom 11. Juli2019 (BGBl. I S. 1066) geändert worden ist* | 3 Europäische Kommission (2017), *Vorschlag für eine Verordnung des europäischen Parlaments und des Rates* | 2 Voraussichtliches Inkrafttreten

Abbildung 9: Konfliktäre Ausgestaltung der Datenschutzgesetzte – ePVO als Abhilfe

Gemäß Artikel 5 Abs. 3 Entwurf der ePVO sei eine informierte Einwilligung auf Basis klarer und umfassender Information über Zwecke der Verarbeitung unbedingt erforderlich. Sollte das TMG dem Entwurf der ePVO folgen, wird ein Opt-In für alle datendiensterelevanten Tags[11] kodifiziert. Die Einwilligung selbst wird dann die Bedingungen von Artikel 7 DSGVO erfüllen müssen, wie zum Beispiel die Nachweisbarkeit der erteilten Einwilligung.

Neben bereits bestehenden Regelungen müssen Vorkehrungen für zukünftige additive Vorgaben der ePVO getroffen werden

Nun hat der Bundesgerichtshof mit dem Urteil Nr. 067/ 2020 vom 28.05.2020 zur Einwilligung in telefonische Werbung und Cookie-Speicherung entschieden, dass zumindest für Cookies, die der Erstellung von Nutzerprofilen für Zwecke der Werbung und Marktforschung sowie bedarfsgerechten Gestaltung von Telemedien dienen, Einwilligungen der Nutzer eingeholt werden müssen. Ein Banner ist nicht mehr ausreichend. Problematisch ist, dass die Verabschiedung der ePVO seit über zwei Jahren anhängig ist und sich die finale rechtliche Ausgestaltung nur vermuten lässt, ihr Ausgang aber Auswirkung sowohl auf Technik als auch insbesondere auf das Geschäftsmodell der Unternehmen haben wird. Innerhalb der gegenwärtigen Debatten wird vor allem die Auswirkung auf die Technik in den Vordergrund gestellt. Sicherlich wird es bei den Tags zur personalisierten oder pseudonymen Identifizierung neue Techniken des Erkennens von Nutzern, der Attribution der Redirect-Kette und des Targetings als letzten Schritt vor der Auslieferung von Werbung geben. Doch das ist letztlich obsolet, denn die Techniken werden in Zukunft ohne

[11] Tags sind 1st, 2nd und 3rd Cookies, JavaScript ID als Session Cookie, Evercookies, Customer ID, Device/Behavioral Fingerprinting, ID Konsortien etc.

Einwilligung des Nutzers rechtlich allesamt gleich als „invasives Tracking“ behandelt und bereits jetzt werden Lösungen in Form von z.B. Consent-Management-Plattformen gefunden und etabliert. So sollte sich die Debatte vielmehr auf die ungewissen Auswirkungen für das Geschäftsmodell der Unternehmen verlagern. Denn was folgt daraus für das Geschäftsmodell der Online-Werbeindustrie, wie zum Beispiel der Medienhäuser?

Fokus auf Lösung technischer Fragen nicht ausreichend für kommende Regelungen der ePVO

In diesem Zusammenhang herrscht Ungewissheit sowohl bei Unternehmen als auch bei Regulatoren. Das Bayerische Landesamt für Datenschutzaufsicht spricht sich wirtschaftsfreundlich aus: Setzt sich die Zielrichtung der DSGVO durch, so müssen auch die Interessen der Verantwortlichen anerkannt werden, was im Umkehrschluss bedeuten würde, es gäbe kein Recht des Nutzers auf freie und kostenlose Nutzung einer Webseite. Dagegen steht die Auffassung der Schwesterbehörde aus Baden-Württemberg, hernach die Erbringung einer Leistung eben nicht an die Verarbeitung von Daten gekoppelt werden darf.[12] Interessant ist diesbezüglich die Auffassung der europäischen Artikel-29-Arbeitsgruppe zu Nachrichtenmedien[13]: „Es besteht eine klare demokratische Notwendigkeit, das wirtschaftliche Überleben der Nachrichtenmedien sicherzustellen. Die Europäische Kommission sollte jedoch nicht akzeptieren, dass Nachrichtenmedien zwangsweise invasives Tracking von Nutzern einführen.“ Ergo sollen Nachrichtenmedien überleben, jedoch nicht mit Tracking. Am Kiosk wird ein Printmedium selbstverständlich bezahlt, im Cyberraum setzt das Publikum die kostenlose Nutzung voraus.

Auf lange Sicht gibt es weitaus mächtigere Gegenspieler der Online-Werbeindustrie und auch der Europäischen Regulierung und Aufsicht: die Browser (-hersteller). Schon heute blocken alle gängigen Browser Third Party Cookies und zum Teil sogar First Party Cookies. Die europäische Politik vertraut Browserherstellern (somit im europäischen Markt im wesentlichen GAFAM) immer mehr Privacy-Funktionalitäten an. Darf ein Unternehmen noch selbst über eine Consent-Management-Plattform seine Nutzer und Kunden bedienen oder wird ihm diese Steuerungsmöglichkeit vom Browser des Nutzers abgenommen? Die Zugangsschranke wird von den Inhaltsherstellern zu den Browsern als Gatekeeper verschoben. Kann Werbung mit dem Vorliegen einer Einwilligung ausgespielt werden oder nicht, so können auch die Inhalte selbst kontrolliert werden. Ist das ein wünschenswertes Vorgehen für die europäische Wirtschaft insgesamt? Wird damit nicht an der Souveränität der selbstständig und frei handelnden Wirtschaftsunternehmen und letztendlich Europas gerüttelt?

Geschäftsmodell mit Einwilligung des Nutzers erfolgsversprechender als gegen den Nutzer

Übergeordnet sollte jedoch vor allem eine zentrale Frage gestellt werden: Wie lange ein Geschäftsmodell gegen den Willen der Nutzer erfolgreich sein kann. Oder ist die Wirtschaft nicht erfolgreicher mit einem aufgeklärten Kunden, der Herr über seine Einwilligung ist? Datendienste mit Einwilligung sind zumal besser als Datendienste ohne Einwilligung, da sie genauer sind. Gleichzeitig hat die Angst vor einer möglichen Überwachung denselben Effekt wie die tatsächliche Überwachung. Insofern sollte der Nutzer durch guten Inhalt, nutzbringende Dienste etc. zu einer Einwilligung überzeugt werden. Den Effekt der immerwährenden Selbstoptimierung der Nutzer (vgl. Wollen → Können[14]) kann nicht ignoriert, sondern muss akzeptiert werden. Produkte und Services müssen entsprechend

[12] Bundesverband Deutscher Zeitungsverleger e.V., (2019), 05.12.2019.

[13] European Commission (2016).

[14] COREresearch (2015), Whitepaper: Wollen → Können.

gestaltet und dem Nutzer zur Verfügung gestellt werden. Es bedarf geeigneter Lösungen, hierin integriert den Wert der Nutzerdaten transparent zu machen und eine informierte, souveräne Entscheidung zur Einwilligung in die Nutzung der Daten durch den Dateneigentümer zu ermöglichen.

Die Summe der Fragen und möglichen Antworten steht sinnbildlich für die Verunsicherung der Unternehmen. Klar ist, ein sicherer Umgang mit Datenschutz wird zunehmend wichtiger, denn mit jeder weiteren datenschutzrechtlichen Entwicklung wird die Komplexität rund um Datenschutz erhöht und sie fordert eine technische Umsetzung sowie ggf. die Anpassung des eigenen Geschäftsmodells.

Exkurs: Möglicher Denkanstoß für die Nutzung von Daten durch Medienhäuser (übertragbar auch auf Szenarien in anderen Industrien) im Rahmen der ePVO – Geschäftsmodelle

Eine Ausgestaltung des Angebotes könnte sich in die Kategorien Basic, Eco, Comfort und Premium gliedern

- *Basic:* Hierbei besteht der für den Nutzer frei zugängliche Inhalt aus einer Grundversorgung (abgeleitet aus dem Versorgungsauftrag von ARD und ZDF)
- *Eco, Comfort und Premium:* Hier wird die Grundversorgung um zusätzliche Inhalte ergänzt, diese können beliebig je nach Angebot Eco, Comfort bis hin zu Premium ausgestaltet werden. Die Grundidee besteht darin, dass zusätzliche Inhalte bezahlt werden müssen, entweder monetär oder mit Daten

Der Grundversorgungsinhalt kann vom Anbieter gänzlich kosten- und datenfrei gestellt werden, oder aber durch pseudonymes First Party Tracking (Werbung passend zu konsumierten Beiträgen) bezahlt werden. Weitere Inhalte werden mit pseudonymem Tracking durch First und Third Party bezahlt. Auch diese Bezahlung mit Daten kann entlang des Angebots aufgefächert werden. Monetarisierte Kunden bezahlen nicht mit Datendiensten, es sei denn sie wünschen zum Beispiel personalisierte Werbung durch ihre Zeitung (First Party) und/ oder durch ausgewählte Werbepartner (Third Party) ihrer Zeitung.

3.3 Verschwendung von Potenzialen der Digitalisierung aus Angst vor Strafen und strategischer Fehlbewertung von Datenschutz

Die im vorherigen Kapitel beschriebenen multiplen Herausforderungen aufgrund von fehlendem Wissen zum Datenschutz und die starke Verunsicherung durch weitere ungewisse rechtliche Entwicklungen und selbstbewusster agierenden Datenschutzaufsichtsbehörden münden in einer „Datenschutzohnmacht“ der Unternehmen.

Dies zusammengenommen führt dazu, dass Unternehmen notwendige (digitale) Weiterentwicklungen nicht energisch vorantreiben oder gar unterlassen:

Abbildung 10: Hemmung von Innovationen mangels Know-hows zu Datenschutz

Notwendige Produktinnovationen und eine Weiterentwicklung des Geschäftsmodelles werden aufgrund von Datenschutzbedenken unterlassen

Ob Online Kundenakquise, der Einsatz neuer Technologien wie Künstliche Intelligenz für Analysen von Kundenverhalten, oder der Einsatz von Clouds für effiziente Automatisierung von Prozessen und für Kosteneinsparungen – Innovationen werden durch Bedenken der Unternehmen zum Datenschutz behindert. Produktinnovationen kommen somit verzögert oder gar nicht zum Einsatz. Damit hemmen Organisationen mangels Beherrschung regulatorischer Anforderungen die für den Unternehmenserfolg unabdingbare Weiterentwicklung. Die digitale und zunehmend datenbasierte Entwicklung des Marktes lässt sich nicht aufhalten. Im Umkehrschluss wird die Auseinandersetzung mit und Investition in Datenschutz unabdingbar.

Wir konnten feststellen, dass eine Grundproblematik dabei vor allem in der strategischen Fehlbeurteilung von Datenschutz durch die Unternehmen liegt. Gegenwärtig sind zwei entgegengesetzte Entwicklungen zu beobachten: Einerseits steigt das Datenschutzbewusstsein der Kunden – 78 % der Nutzer sind um den Schutz ihrer Onlinedaten besorgt[15] – „Kunden kaufen nicht mehr bei Marken, die gute Produkte anbieten, sie kaufen bei Marken, denen sie vertrauen“, so die englische Autorin und Oxford-Dozentin Rachel Botsman[16].

[15] Ipsos (2019), S. 8.

[16] FAZ (2019), 01.05.2020.

Die Mehrheit der Unternehmen bewertet Datenschutz strategisch falsch – einige wenige entwickeln Wettbewerbsvorteile aus strategischer Berücksichtigung des Datenschutzes

Andererseits haben die meisten Unternehmen nicht verstanden, welche Bedeutung Datenschutz für ihre Kunden und somit für ihren Erfolg hat. Denn 63 % von 862 befragten deutschen Unternehmen sehen die DSGVO nicht als Chance und Wettbewerbsvorteil[17], obwohl sie auf die Wahrung der von Kunden geforderten Datenschutzrechte abzielt. 47 % betrachten die DSGVO sogar als wettbewerbsschädigend[18], statt sie als Rahmenwerk zur Wiedererlangung des Kundenvertrauens zu verwenden und tatsächlich zu erkennen, welche enorme Rolle Datenschutz mittlerweile für Kunden und andere Stakeholder eigenommen hat.

Diese Zusammenhänge von Kundenvertrauen, Akzeptanz und Datenschutz sind bei erfolgreichen Technologiekonzernen wie Apple und Facebook offensichtlich besser verstanden und verinnerlicht. Denn bei ihnen hat ein Umdenken stattgefunden – immer mehr werben diese Unternehmen mit datenschutzfreundlichen Einstellungen und Produktfeatures, z.B. Apple: „Privacy. That's iPhone."[19]. Sie setzen damit ein Statement, befriedigen damit (zumindest wahrgenommen) das Kundenbedürfnis nach Datenschutz, indem sie sich als vertrauenswürdiger Anbieter etablieren, sie werden u.a. damit durch Kunden bevorzugt.

[17] IWD (2020),01.05.2020.

[18] IWD (2020),01.05.2020.

[19] YouTube (2019) Werbevideo von Apple, 03.05.2020.

4 Anleitung zum souveränen Wettbewerb mit Datenschutz

Unternehmen mit Datenschutz als Strategieelement sehen diverse Wettbewerbsvorteile

Man kann dem Ansatz der meisten Unternehmen folgen und Datenschutz als notwendiges Übel, Bürokratiemonster und Revisionsobjekt sehen oder aber man wählt eine andere Betrachtungsweise und nutzt Datenschutz als Vertrauensanker zum Kunden, Distinktionsmerkmal im Wettbewerb und somit als eine weitere (gleichberechtigte) Grundlage der Ausgestaltung eines nachhaltig erfolgreichen Geschäftsmodells.

Diese Betrachtungsweise haben manche Unternehmen erkannt und sehen diverse Vorteile in der Konformität zum Datenschutz:

Unternehmen sehen Vorteile in der DSGVO-Konformität

Quelle: Cisco (2019), *Data Privacy Benchmark Study* | Anmerkung: Prozentzahl gibt an, wie viel % der befragten Unternehmen die genannten Vorteile sehen

Abbildung 11: Datenschutz bietet Vorteile

Die Chancen des Datenschutzes fokussierend, stellen wir zunächst ein Vorgehensmodell in drei Stufen vor, mit dessen Hilfe ein Unternehmen sowohl konform zur DSGVO wird als auch Vorteile im Wettbewerb durch vertrauensbildenden Datenschutz generieren kann.

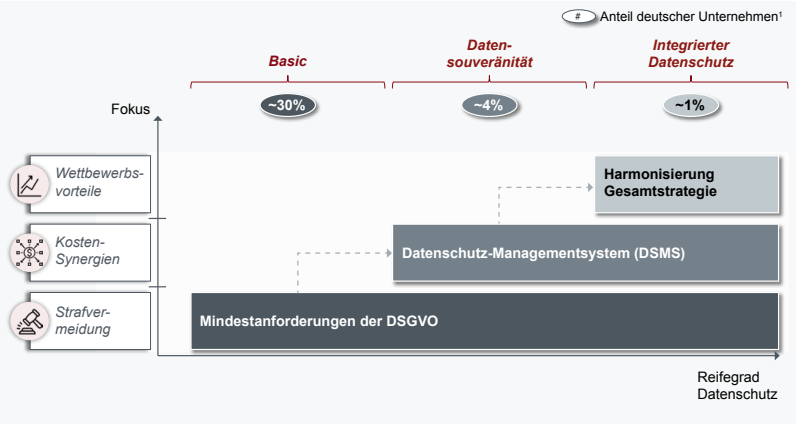
Moderner Datenschutz erfordert technologisch gestaltete Datensicherheit. Natürlich können Datenschutz und Datensicherheit auch manuell umgesetzt werden, jedoch nicht zu wettbewerblichen Eigenschaften und Kosten. Hierfür zeigen wir die Vorteile moderner IT-Architekturen, auch für den Datenschutz, auf. Im letzten Teil dieses Kapitels geben wir Erfahrungen aus unserer Umsetzungspraxis, welche einerseits Sachverhalte kompakt erklären und anderseits Arbeitsanweisungen zur Durchführung geben.

4.1 3-Stufen-Modell – Konformität, Souveränität, Integrität

Das Ambitionsniveau bei der Erfüllung von Datenschutzanforderungen kann sich je nach Ziel einer Organisation unterschiedlich gestalten. Während manche Unternehmen den Anspruch definieren, eine bloße Datenschutzkonformität zu erreichen, werden andere Unternehmen einen Mehrwert mit Daten und Datenschutz erzielen wollen. Hierfür haben wir ein Vorgehensmodell erarbeitet, das drei Ambitionsniveaus beinhaltet. Das 3-Stufen-Modell gliedert sich in Basic, diese Stufe stellt bei jeglicher Geschäftstätigkeit Gesetzeskonformität her. In der zweiten erlangt das Unternehmen souveränen Umgang mit Datenschutz, um in der dritten Stufe die Datenschutzstrategie als integralen Bestandteil der Gesamtstrategie ein-

zubetten und damit Datenschutz als Produkt und Service am Markt anzubieten.

Transformation in 3 Stufen zur Integration des Datenschutzes in die Unternehmensstrategie



Quelle: COREresearch (2020) | 1. Expertenschätzung COREresearch (2020)

Abbildung 12: 3-Stufen-Modell für nachhaltigen Datenschutz

3-Stufen-Modell zur individuellen Entwicklung des Datenschutzes im Unternehmen

- Die erste Stufe „Basic“ dient der Herstellung von Konformität zur DSGVO, d.h. der Gesetzestreue. Mit dem Durchlaufen der Stufe können Sanktionen aus Datenschutzvergehen effizient vermieden werden
- Endprodukt der zweiten Stufe ist ein Datenschutz-Managementsystem (DSMS) und damit die Erwirtschaftung von Ertrag aus Daten mittels souveränen Umgangs mit diesen. Nebenbei erlangt das Unternehmen auch eine Zertifizierungsfähigkeit des Datenschutzes
- In der letzten Stufe wird Datenschutz zum integralen Bestandteil der Gesamtstrategie und es werden Wettbewerbsvorteile, Synergieeffekte und somit die Beherrschung des Zukunftsfeldes datengetriebener Geschäftsmodelle erreicht

Je nach Datenschutzreifegrad werden verschiedene Startpunkte zu wählen sein. Zu betonen ist, dass alle drei Stufen aufeinander aufbauen und z.B. Vorteile der dritten Stufe nur mit dem Durchlaufen der ersten und zweiten realisiert werden können.

4.1.1 Basic – Ergebnis: Konformität

Basis ist die effiziente Sicherstellung der gesetzlichen Mindestanforderungen

Mit Basic kennt das Unternehmen die verarbeiteten personenbezogenen Daten und wird dadurch in die Lage versetzt, die notwendige gesetzliche Pflichterfüllung zu gewährleisten. Dazu nennt die DSGVO zehn wesentliche Punkte:

Mindestbestandteile zur Erlangung der Datenschutzkonformität gemäß DSGVO

Quelle: Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) in der aktuellen Version des ABl. L 119, 04.05.2016

Abbildung 13: Mindestbestandteile einer Datenschutzkonformität gemäß DSGVO

DSGVO-Konformität als Checkliste

Im Rahmen der Kontrollfunktion ist ein Datenschutzbeauftragter (DSB) zu ernennen und an die zuständige Landesdatenschutzbehörde zu melden. Dieser agiert in Datenschutzthemen nicht weisungsgebunden und ist für die Erfüllung aller Aufgaben aus Artikel 39 DSGVO verantwortlich. Dazu zählen in praxi unter anderem die Erstellung einer Datenschutzrichtlinie, ein Verzeichnis über die Verarbeitungstätigkeiten und ein Löschkonzept. Dieses umfasst unter anderem die Zurverfügungstellung einer Auflistung aller Tätigkeiten mit Aufbewahrungsfrist oder Löschfrist und macht Aussagen zum Umgang mit Backups und Archiven. Weiter verantwortet der DSB die Prüfung des Erfordernisses und wenn nötig die Durchführung einer Datenschutz-Folgenabschätzung, die Sicherstellung der technisch-organisatorischen Maßnahmen und die Erfüllung der Betroffenenrechte. Auch liegt in dessen Verantwortung die Erstellung und Umsetzung eines dedizierten Konzepts zum Umgang mit Betroffenenrechten, das einen Bestandteil von umfassenden Schulungen aller Mitarbeiter darstellt. Letztlich ist im Rahmen eines standardisierten Vorgehens das Erfordernis und mögliche Umsetzung von Auftragsverarbeitungen zu prüfen.

Basic wird in den meisten Fällen ex post angewendet werden müssen, um zunächst einmal Gesetzeskonformität zu erlangen und so Sanktionen aus Datenschutzverletzungen zu vermeiden. Basic kann auch von vornherein Anwendung finden. Für diese ex tunc Anwendung ist allerdings ein Managementsystem prädestiniert. Mit Basic wird neben Datenschutzkonformität auch der Grundstein für das Datenschutz-Managementsystem der zweiten Stufe gelegt.

Aus den o.g. zehn wesentlichen Punkten werden nachfolgend zu den vier absoluten Pflichtdokumenten Hinweise aus unserer Expertise und praktischen Erfahrung zu ihrer Erstellung gegeben. Diese Dokumente sind in der regulatorischen Theorie wohl definiert, bürgen aber etliche Umsetzungshindernisse.

Die vier Dokumente sind

- Verzeichnis der Verarbeitungstätigkeiten
- Löschkonzept
- TOM-Dokument
- Prüfung der Erforderlichkeit der Durchführung einer Datenschutz-Folgenabschätzung

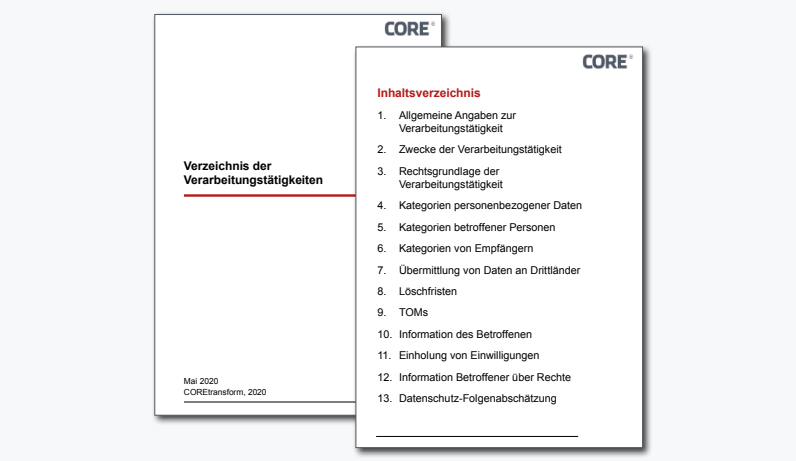
Verarbeitungsverzeichnis steuert notwendige Dokumentation und erfüllt additiv Rechenschaftspflichten der DSGVO

Keine Angst vor dem Verarbeitungsverzeichnis

Im Falle eines Datenschutzaudits wird die Aufsichtsbehörde erstens das Audit mit einer Woche Vorlauf ankündigen und zweitens das Verarbeitungsverzeichnis sofort zur Einsicht verlangen. Die exakte Übereinstimmung des Verarbeitungsverzeichnisses mit der Datenschutzrealität in dem auditierten Unternehmen ist nicht von höchster Relevanz, es kommt vielmehr darauf an, ein plausibles Verarbeitungsverzeichnis vorlegen zu können, welches aktuell ist und erkennen lässt, dass der Verantwortliche methodisch, umfassend und buchstäblich verantwortungsbewusst Datenschutz in der Praxis des Unternehmens umsetzt. Ein gutes Verarbeitungsverzeichnis legt den Grundstein für alle weiteren Dokumente, insbesondere für Löschkonzept und die technisch-organisatorischen Maßnahmen.

Ein hervorragendes Verarbeitungsverzeichnis dokumentiert darüber hinaus nicht nur die Mindestinhalte gemäß Artikel 30 DSGVO, sondern auch alle sich aus weiteren Artikeln ergebenden Pflichten, um Rechenschaft über die Rechtsgrundlagen der Verarbeitungstätigkeit abgeben zu können, wie zum Beispiel Speicherbegrenzung und Betroffenenrechte. So besteht der Fragenkatalog pro Verarbeitungstätigkeit nicht nur aus Vorblatt und 8 Mindestfragen, sondern aus 13 Fragen:

Template zur Erstellung von einem Verarbeitungsverzeichnis



Quelle: COREresearch (2020)

Abbildung 14: Struktur für Verarbeitungsverzeichnis

Trennung des Löschkonzeptes für Organisation und Anwendung verschafft Herrschaft über das Löschen zurück

Unsere Erfahrung zeigt, dass sich für datengetriebene Unternehmen eine Zweiteilung des Löschkonzepts in Organisation und Anwendung empfiehlt. Der Organisation kommt dabei die Rolle des Betreibers der Anwendung zu. In der Organisation werden Sanktionen aus Datenschutzvergehen vermieden, in der Anwendung wird mit Datenschutz Nutzen erwirtschaftet. Das Maß aller Löschkonzepte ist die DIN-Norm 66398 („Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“). Die Entwicklung zum Löschkonzept wird in den folgenden Schritten beschrieben:

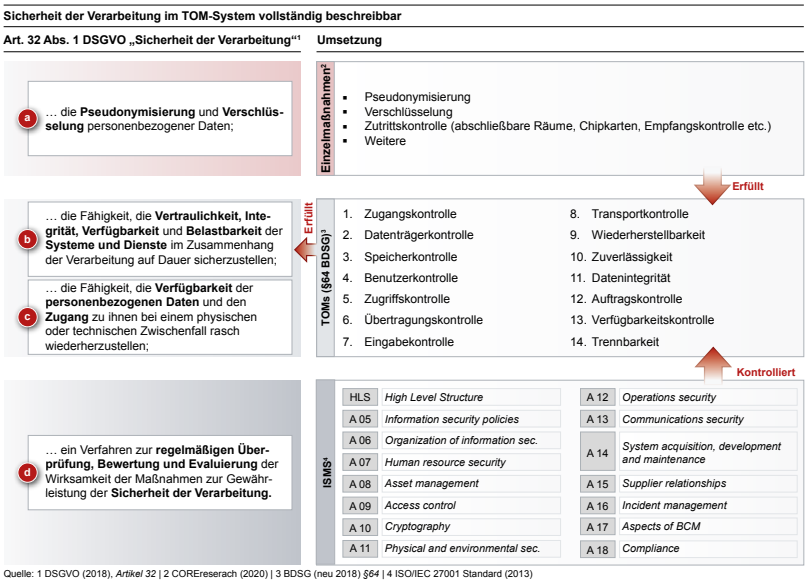
- Bestimmung der Datenarten
- Bestimmung der Standardlöschfristen
- Identifizierung der Startzeitpunkte
- Bildung von Löschklassen
- Umsetzung Löschprozesse

Für die Organisation empfiehlt sich der Aufbau einer Tabelle mit den wesentlichen Gesetzen für Aufbewahrungspflicht und Löschgeschehen wie § 147 AO, § 257 HGB, §§ 195 und 199 BGB, Artikel 6 und Artikel 17 DSGVO und § 26 BDSG für Löschfristen und den abzuleitenden Startzeitpunkten. Für die Anwendung und ihre zumeist wenigen verarbeiteten personenbezogenen Datenarten kann dann konkret die Löschklassentabelle gemäß DIN 66398 aufgebaut werden.

Technisch-organisatorische Maßnahmen (TOM) sind abzählbar und automatisierbar

Das TOM-Dokument beschreibt alle Maßnahmen zur Sicherheit der Verarbeitung der personenbezogenen Daten. Gemäß Artikel 32 DSGVO müssen Verantwortliche und Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen zum Schutz von personenbezogenen Daten treffen. Im Gesetz werden als Maßnahmen genannt:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung



Quelle: 1 DSGVO (2018), *Artikel 32* | 2 COREreserach (2020) | 3 BDSG (neu 2018) *§64* | 4 ISO/IEC 27001 Standard (2013)

Abbildung 15: System der technisch-organisatorischen Maßnahmen (TOM)

Best-Practices bieten geeignete Vorlagen für ein automatisierbares TOM-System

Damit enthalten Artikel 32 DSGVO i.V.m. §64 BDSG alle Komponenten zur Aufstellung eines TOM-Systems, sodass sich 14 technisch-organisatorische Maßnahmen ergeben, welche konkret durch Einzelmaßnahmen umgesetzt werden. Die Menge der Kombinationsmöglichkeiten aus TOM und Einzelmaßnahmen ist endlich, sodass das TOM-System vollständig beschrieben und automatisiert werden kann. Auch die vierte Anforderung aus Artikel 32 DSGVO, das „Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM …“ ist bei einem gut aufgestellten Verantwortlichen in Form eines Informationssicherheits-Managementsystems (ISMS) bereits vorhanden. Als Ergebnis kann ein TOM-System wie in Abbildung 15 skizziert aufgestellt werden, das sowohl zum Beleg der eigenen Maßnahmen als auch für Auftragsverarbeitungsverträge genutzt werden kann.

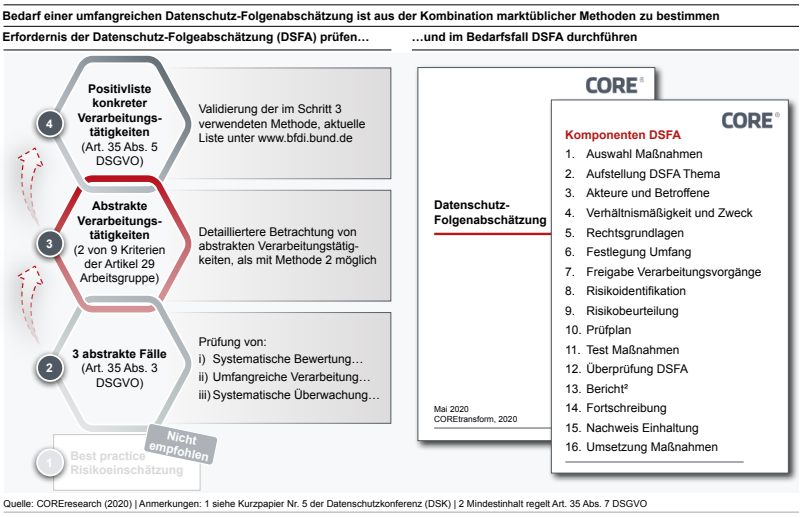
Erfordernis einer Datenschutz-Folgenabschätzung kann nach Katalog vorabgeprüft werden

Datenschutz-Folgeabschätzung nur anzuwenden, wo sie wirklich erforderlich ist, weitgehende Vermeidung möglich

Eine Datenschutz-Folgenabschätzung (DSFA) muss durchgeführt werden, wenn eine vorgesehene Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Hierzu muss der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungstätigkeiten für den Schutz personenbezogener Daten durchführen. Gesetzgeber und Aufsichten bieten insgesamt vier Methoden an, welche sich zu einem strukturierten Vorgehensmodell für die DSFA-Vorabprüfung entwickeln lassen. Die erste Methode ist der „Klassiker" des Risikomanagements: eine Matrix aus Eintrittswahrscheinlichkeiten und potenziellen Schadenshöhen. Es folgen

- Drei abstrakte Fälle aus Artikel 35 Abs. 3 DSGVO
- „2 aus 9 Kriterien"-Methode der Artikel-29-Arbeitsgruppe mit der Nennung von neun abstrakten Verarbeitungsvorgängen
- Positivliste der Verarbeitungstätigkeiten der Datenschutzkonferenz mit der Nennung von 17 konkreten Verarbeitungsvorgängen

In der Theorie reicht die Prüfung des Erfordernisses einer DSFA nach nur einer Methode. In der Praxis ist es dann doch komplizierter: Wir empfehlen, die Matrixmethode nicht zu verwenden und nach den drei verbliebenen Methoden zu prüfen. Ergeben alle drei Methoden ein Nein, ist keine vollumfängliche DSFA notwendig.



Quelle: COREresearch (2020) | Anmerkungen: 1 siehe Kurzpapier Nr. 5 der Datenschutzkonferenz (DSK) | 2 Mindestinhalt regelt Art. 35 Abs. 7 DSGVO

Abbildung 16: Prüfung einer DSFA ist methodisch strukturiert durchführbar

4.1.2 Datensouveränität durch ein Datenschutz-Managementsystem

Während im ersten Schritt vor allem eine nach außen gerichtete DSGVO-Konformität erreicht wird, gilt es im zweiten Schritt eine langfristige Konformität von innen heraus aufzubauen. Mit dem Durchlaufen der ersten Stufe werden hierfür zwar die notwendigen Bausteine als „Basis" gelegt, jedoch zumeist „noch" nicht im Unternehmen manifestiert.

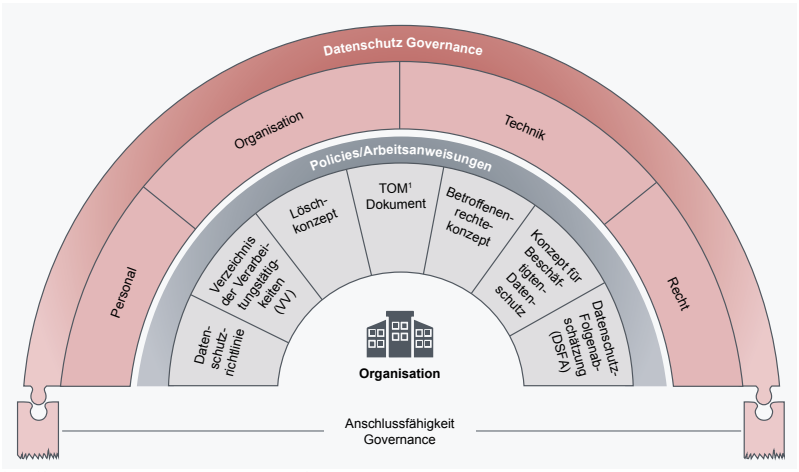
Ein System, welches Einzelmaßnahmen und einzelne Datenschutzprozesse harmonisiert sowie Policies tatsächlich umsetzt, wird von Nöten sein.

Das Datenschutz-Managementsystem (DSMS) legt fest, mit welchen Instrumenten und Methoden die Leitungsebene einer Institution die auf Datenschutz ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenken kann. Ein DSMS unterstützt somit das eigene Ambitionsniveau im Datenschutz zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Erst durch die Einführung eines DSMS wird gewährleistet, dass Datenschutzkonformität tatsächlich nachhaltig durch die eigene Organisation umgesetzt werden kann.

Das Datenschutz-Managementsystem harmonisiert die Summe aller Datenschutzprozesse und -belange einer Organisation

Durch die Schaffung eines DSMS wird Datenschutz nun als geschlossenes (Management) System betrachtet, sodass die Anschlussfähigkeit an andere Managementsysteme, wie z.B. das Informationssicherheits-Managementsystem und dessen dazugehörige Strategie einfacher möglich ist. Einzelne Komponenten, wie zum Beispiel „Basic"-Datenschutzkomponenten, können aufgrund der übergeordneten Steuerung nun gezielt kraftschlüssig miteinander über diverse Managementsysteme hinweg kombiniert werden.

Empfohlener Aufbau und Anschlussfähigkeit eines Datenschutz-Managementsystems (DSMS)



Quelle: COREresearch (2020) | 1: Technische und organisatorische Maßnahmen

Abbildung 17: Bestandteile eines Datenschutz-Managementsystems (DSMS)

Die beschriebene übergeordnete Steuerung wird mittels einer Erweiterung des skizzierten Datenschutz-Mindestsetups von „Basic" in allen Dimensionen durch die Etablierung einer Datenschutz-Governance erreicht. Diese besteht aus vier übergreifenden Ebenen: Personal (personelle Aufstellung), Organisation (Aufbau- und Ablauforganisation), Technik mit darunter subsummierten technischen Maßnahmen und Recht (juristische Perspektive).

Das DSMS entfaltet seine Wirkung auf vier Ebenen: Personal, Organisation, Technik und Recht

Wichtig ist dabei, dass keine Ebene allein für sich stehen kann und sie nur gemeinsam ihre volle Zielwirkung entfalten können. Deshalb empfehlen wir die Ebenen schrittweise parallel aufzubauen – sollten sie nicht bereits vorhanden sein. Folglich soll die Reihenfolge der Nennung der vier Ebenen keinesfalls eine Priorisierung darstellen. Uns ist bewusst, dass das erwünschte Ambitionsniveau nicht „von heute auf morgen" erreicht werden kann, deshalb werden im Rahmen der Erklärung ausgewählte Elemente des DSMS vorgestellt, die für den Aufbau von zentraler Bedeutung sind und selbstverständlich individuell an die Zielorganisation angepasst und ergänzt werden können und müssen.

Personal

Die wichtigste personelle Besetzung im Kontext des Datenschutzes ist der/ die Datenschutzbeauftragte (DSB), ob intern oder extern spielt dabei vordergründig nur für Kündigungsfristen und Haftung eine Rolle. In den meisten Unternehmen ist die Rolle mittlerweile besetzt und in der Regel benannt, jedoch nicht aktiv eingesetzt. Der DSB wird zumeist zu spät oder gar nicht in Entscheidungsprozesse einbezogen. Da viele Organisationen nicht die Notwendigkeit des Einbeziehens des DSBs in Entscheidungsprozesse erkennen oder Schwierigkeiten haben – vor allem bei Externen – diese einzubeziehen, empfiehlt es sich den DSB um zwei zusätzliche datenschutzrelevante Akteure zu ergänzen: Dem Datenschutz-Ambassadeur und -Koordinator.

Die Benennung von Datenschutz-Ambassadeuren und -Koordinatoren ermöglicht eine End-2-End-Verantwortung im Datenschutz

Während der Datenschutz-Ambassadeur vor allem für technische Themenstellungen, wie der Einhaltung von Privacy-by-Design zur Unterstützung in der Umsetzung von konkreten IT-Lösungen eingesetzt wird, kommt dem Datenschutzkoordinator eine übergreifende Funktion zu. Dieser dient als „Schnittstelle“ und „Sprachrohr“ des DSB in einzelne Abteilungen einer Organisation und trägt so dazu bei, dass notwendige Datenschutzbelange trotz Abwesenheit des DSBs in die Organisation getragen und umgesetzt werden. Wir empfehlen auch, dass alle genannten Rollen in enger Zusammenarbeit mit dem Informationssicherheitsbeauftragten (ISB) agieren, um Datensicherheit zu gewährleisten. Möchte man darüber hinaus eine konstante „Management-Attention“ auf das Thema Datenschutz erreichen, ist ein möglicher Lösungsansatz, Datenschutz durch direkte/ indirekte Vertretung in der Geschäftsleitung durch ein Leitungsmitglied mit entsprechendem Know-how oder durch enge Einbindung der Kontrollfunktion Datenschutz auf oberster Führungsebene des Unternehmens zu manifestieren.

Organisation

Sind die personellen Grundsteine gelegt, gilt es Datenschutz in Form eines „Datenschutzausschuss“ zu instanziieren. Ähnlich wie bei einem IT- oder Risikoausschuss sollte dieser mindestens einmal im Quartal tagen sowie ad hoc bei Auftreten von Vorfällen oder wichtigen Diskussionspunkten zusammentreten. Empfehlenswert ist eine (Mindest-)Zusammensetzung aus Geschäftsleitung, DSB, ISB und Risikomanager sowie Recht und bei Bedarf Personal. Entscheidungen und Ziele des Gremiums sollten regelmäßig in die Organisation kommuniziert werden und zur Durchsetzung mit End-2-End-Veratwortlichen versehen werden.

Instanziierung durch Datenschutzausschuss notwendig für effektive und effiziente Implementierung organisatorischer Maßnahmen

Zu notwendigen organisatorischen Maßnahmen gehört die Sicherstellung der Umsetzung von Datenschutz. Diese wird nicht durch bloßes „Abheften“ und Verkünden von Datenschutzpolicies als Rahmenwerke für alle Datenschutzaktivitäten erreicht. Um wichtige Datenschutzprozesse im Unternehmen zu manifestieren und damit Datenschutzfehler nachhaltig zu behandeln, müssen Richtlinien und Arbeitsanweisungen zunächst in Prozesse übersetzt und in regelmäßigen Workshops mit Mitarbeitern verprobt werden. In Workshops werden Prozesse nicht nur von betroffenen Mitarbeitern nachvollzogen, sondern zumeist können hierdurch Verbesserungspotenziale und überflüssige Prozesse oder Prozessschritte identifiziert und angepasst werden. Anpassungen sind im Prozessverzeichnis zu dokumentieren. Vorzugsweise werden Workshops zu Beginn halbjährlich und dann jährlich durchgeführt.

Im zweiten Schritt werden die Policies erweitert. Die Datenschutzrichtlinie wird um eine Datenschutzleitlinie ergänzt. Diese ist vor allem als Bekenntnis der Unternehmensleitung zum Datenschutz nach außen an Kunden, Partner und Aufsicht gerichtet. Hinzu kommt das Vertragsverzeichnis, welches wesentliche Verträge zu Auftragsverarbeitung, Sicherheit der Verarbeitung oder Drittstaatenregelung überprüft. In der Lieferantenrichtlinie werden Datenschutzanforderungen an Lieferanten und die Sourcing-Strategie berücksichtigt. Je nach Schwerpunkt des Geschäfts können weitere Aspekte des Datenschutzes, wie zum Beispiel Cookies, Backups oder Consent-Management in zusätzlichen Policies ausgelagert werden.

Erst durch die Übersetzung von Policies und Durchführung von Workshops wird die Umsetzung von Datenschutz in der Organisation manifestiert

Technik

Technisch gilt es, vor allem Datenschutzprozesse möglichst effizient zu stützen und sämtliche Prozesse auf Datenschutzbedarfe zu überprüfen. Können Löschfristen technisch umgesetzt werden? Werden notwendige Prinzipien wie Privacy-by-Design und Privacy-by-Default eingehalten? Privacy-by-Design kann z.B. durch eine IT-Infrastruktur mit zuschaltbarer Verschlüsselung at rest und at transport sowie Pseudonymisierung erreicht werden. Privacy-by-Default wird durch datenschutzfreundliche Voreinstellungen wie Opt-in oder Consent-Management-Lösungen realisiert. Bei der Umsetzung und Identifizierung notwendiger technischer Maßnahmen hilft der Datenschutz-Ambassadeur.

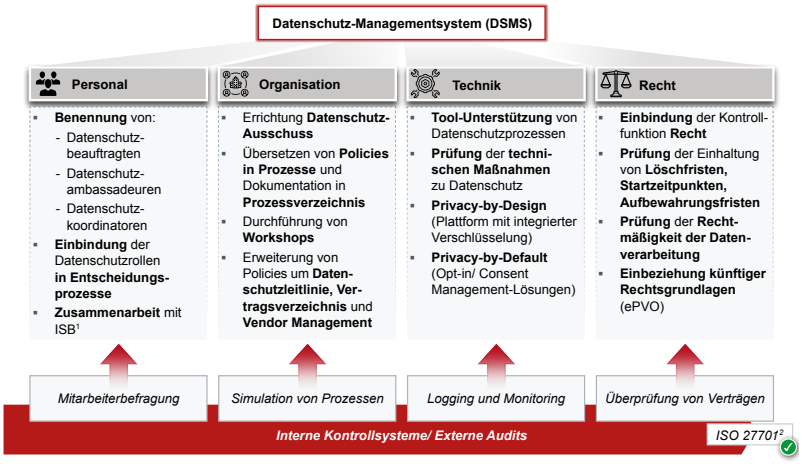
Recht

Aufgrund der zumeist empfundenen Komplexität des Datenschutzes ist neben der engen Zusammenarbeit mit dem DSB und ISB auch die Zusammenarbeit mit der Rechtsabteilung zu empfehlen. Denn Prüfpunkte, wie Kontrolle aller wesentlichen Verträge und Prozesse, Einhaltung von Löschfristen, Startzeitpunkten, Archivierungsdauern und dem Vorhandensein einer Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten, können hierdurch gewährleistet werden. Im Rahmen dieser Ebene gilt es, auch künftige Regelungen wie die ePrivacy-Verordnung zu berücksichtigen und in die anderen Ebenen zu übertragen.

Die Kombination mit juristischer Expertise hebelt TOM zur umfassenden Datenschutzkonformität

Zusammenfassend empfehlen wir, folgende Aspekte zum Aufbau eines DSMS zu berücksichtigen:

Wesentliche Maßnahmen zum Aufbau eines Datenschutz-Managementsystems und Erreichung der Zertifizierungsfähigkeit



Quelle: COREresearch (2020) | 1 Informationssicherheitsbeauftragter | 2 Zertifizierungsfähigkeit auf Basis einer Zertifizierung nach ISO 27001

Abbildung 18: Maßnahmen zum Aufbau eines zertifizierungsfähigen DSMS

Das Datenschutz-Managementsystem für höhere Souveränität im Umgang mit Daten – Grundlage für externe Zertifizierung

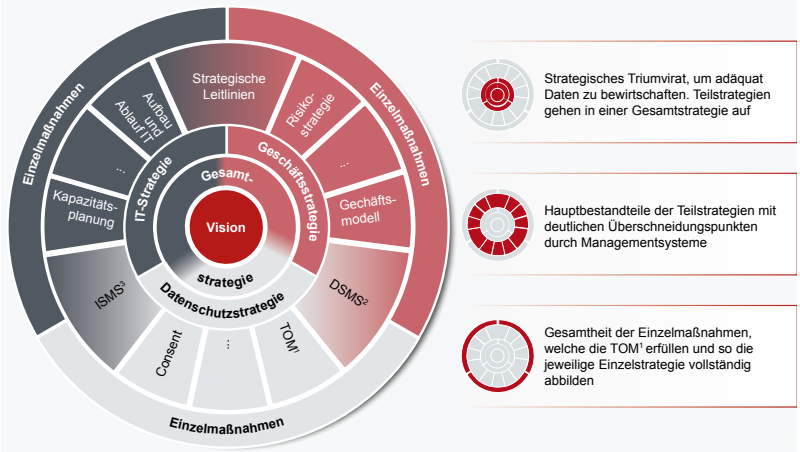
Zusätzlich raten wir über alle Ebenen hinweg zur Messung der Funktionsfähigkeit des DSMS mit Ableitung von Verbesserungspotenzialen. Hier können Standards wie die ISO 27004 herangezogen werden. Mit dem Aufbau eines DSMS wird das Unternehmen nicht nur zum Souverän der Nutzung des Datenschutzes im Wettbewerb, sondern es erlangt „nebenbei“ die Zertifizierungsfähigkeit im Datenschutz. Eine Zertifizierung gemäß DSGVO ist derzeit noch nicht möglich, da für eine offizielle DSGVO-Zertifizierung noch Genehmigungsentscheidungen der europäischen Regulierungsbehörden ausstehend sind. Jedoch können sich Unternehmen mit dem neuen ISO-Standard 27701 bereits jetzt bezüglich Datenschutzkonformität prüfen lassen. Voraussetzung dabei ist ein etabliertes Informationssicherheits-Managementsystem (ISMS) gemäß ISO-Standard 27001. Durch die so strukturierte „einfach und sicher“ erlangte Zertifizierungsfähigkeit wird das Fundament für die nötige Ausrichtung des Unternehmens und damit aller Mitarbeiter mit der Einleitung eines Kulturwandels zu einem ex tunc Datenschutz in allen unternehmerischen Belangen und zu allen interessierten Parteien – Kunden, Mitarbeiter, Partner und Aufsicht – gelegt.

4.1.3 Datenschutz als integraler Bestandteil der Gesamtstrategie

Datenschutz und Informationssicherheit als Elemente der Gesamtstrategie

Zwar verfügen viele Unternehmen über eine Geschäftsstrategie und über eine IT-Strategie, beides zum Beispiel im Finanzsektor durch BAIT, VAIT und KAIT aufsichtsrechtlich begründet, zumeist jedoch über keine dedizierte Datenschutzstrategie. Aus unserer Sicht ist dies zur Erzielung möglicher Wettbewerbsvorteile unabdingbar bzw. dringend empfohlen. Die dritte Phase des 3-Stufen-Modells dient der Realisierung einer integrierten Gesamtstrategie durch Harmonisierung der Business-, IT- und Datenschutz-Strategie. Mit dieser Stufe wird Datenschutz im Angebotsportfolio verankert und so zum Geschäftszweck. Die Zertifizierung ist ein Selbstläufer und ein Muss aus dem strategischen Selbstverständnis des Unternehmens als Datensouverän heraus. Das Unternehmen positioniert sich als strategischer Vertrauenspartner für Kunden, sichert langfristig seine Wettbewerbs- und Innovationsfähigkeit unter Beibehaltung notwendiger Effizienz durch Synergieeffekte aus der Harmonisierung seiner Strategien.

Kombination der 3 Teilstrategien, Geschäfts-, IT- und Datenschutzstrategie zu einer Gesamtstrategie



Quelle: COREresearch (2020) | 1 Technische und organisatorische Maßnahmen I 2 Datenschutz-Managementsystem I 3 Informationssicherheits-Management-System

Abbildung 19: Integration von Geschäftsstrategie, IT-Strategie und Datenschutzstrategie zur Gesamtstrategie

Datenschutz kann nun als Hebel für Wettbewerbsvorteile und zur langfristigen Aufrechterhaltung der Flexibilität und Innovationsfähigkeit genutzt werden. Das Vorhaben lässt sich auf das Mantra „Man muss Datenschutz leben, um Datenschatz zu heben“ verkürzen.

Das Sortieren der eigenen Ambitionen hinsichtlich Geschäftszielen, IT-Infrastruktur, Informationssicherheit und Datenschutz muss in einer integrierten Gesamtstrategie des Unternehmens münden, aus der auch das Ziel der Positionierung des Datenschutzes im Wettbewerb hervorgeht.

Harmonisierung von Datenschutz mit Geschäfts- und IT-Strategien zu einer Gesamtstrategie

Harmonisierung individueller Teilstrategien über Datenschutz zu einer Gesamtstrategie

Zuerst werden die Abhängigkeiten und ihre Auswirkungen bei der Verarbeitung personenbezogener Daten zwischen den Stakeholdern Nutzer, Partner, Investoren, Regulatoren, Aufsichten und dem Unternehmen analysiert. Weiter ist ein individuelles Zielbild im Umgang mit personenbezogenen Daten zu definieren und mit den Zielen existierender Strategien zu vergleichen. Durch die Harmonisierung dedizierter Berührungspunkte der Strategien wesentlicher primärer Funktionen wie Produkt, Marketing, Einkauf, IT, Informationssicherheit und Lieferantenmanagement sowie wesentlicher unterstützender Funktionen wie Finanzen, Informationssysteme und Human Resources werden diese Strategien auf die Anwendung fokussiert. Mit dem Entscheid pro Datenschutzkonformität ist die Platzierung zum Nutzer hin als vertrauenswürdiger Partner bereits in der Phase Basic vorausgewählt worden. Das Vertrauensversprechen muss im Folgenden untermauert werden. Für die strategische Positionierung zum Datenschutz werden die genannten Strategien um die Datenschutzstrategie zu einer Gesamtstrategie vereinigt. Datenschutz ist hiernach mit allen anderen strategischen Zielen gleichberechtigt.

Stärkung der Organisation entsprechend der Bedeutung von Datenschutz in der Gesamtstrategie

Data Privacy und Security Ambassadeure als Partner in der IT-Lösungsentwicklung

In Anlehnung an die Gesamtstrategie bedarf es einer Ergänzung der Organisation, um Datenschutz institutionell zu verankern. Die Verankerung und Stellung von Datenschutz auf Ebene der Governance ist neben den gesetzlich vorgeschriebenen Rollen individuell abzustimmen. Relevant ist es jedoch, dass die bereits mit der Stufe Basic eingeführte Rolle des DSB einen festen Sitz in datenschutzrelevanten Gremien erhält. Ergänzende organisatorische Maßnahmen umfassen folgende Aspekte:

- Definition übergeordneter Datenschutzanforderungen durch Data-Privacy-Ambassadeur
- Beratung von Softwareentwicklern zur Umsetzung des Privacy-by-Design durch Security-Ambassadeure als integraler Bestandteil agiler Entwicklungsteams
- Etablierung von Datenschutz-Gilden zum fachlichen Austausch im gesamten Unternehmen

Beide Ambassadeure besitzen Expertise in IT-Sicherheit respektive Datenschutz. Sie fungieren – das ist erfolgskritisch – nicht als Kontrolleure der Entwickler, sondern als Partner.

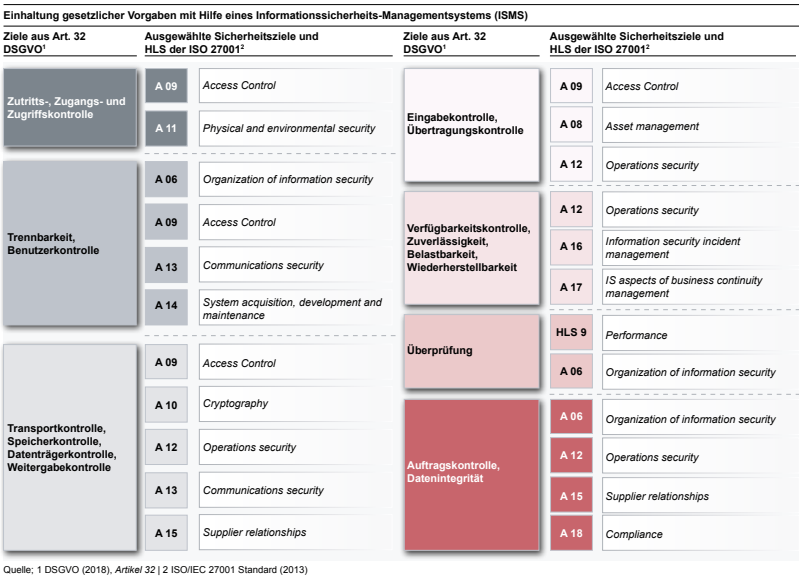
Prozessseitige Harmonisierung

Datensicherheit und Datenschutz sind nicht mehr zu trennen, beide zahlen aufeinander ein

Nach der Harmonisierung der Strategien aller Stakeholder und ihrer Erweiterung um die Datenschutzstrategie sowie der Ergänzung der Organisation folgt im letzten Schritt die Harmonisierung aller relevanten Prozesse auf Datenschutzbelange. Aus den Anforderungen der DSGVO lassen sich eine Vielzahl von prozessualen und IT-seitigen Herausforderungen ableiten. Sie werden z.B. durch veränderte Anforderungen an Datenverarbeitungsprozesse oder die Anforderung zur Umstellung der internen Systemlandschaft repräsentiert. Erschwerend für die Umsetzung des Datenschutzes erweist sich dabei oft eine veraltete IT-Infrastruktur (siehe Kapitel 4.2), denn ohne leistungsfähige und sichere IT ist Datenschutz in einer digitalisierten Welt ein leeres Versprechen.

TOM verbinden Datenschutz mit Datensicherheit

Die Prozesse einer datengetriebenen Unternehmung bestehen aus Geschäftsprozessen und Anwendungsprozessen; die letzteren setzen sich aus Backend- und Frontend-Prozessen zusammen. Einer Gruppe von Geschäftsprozessen kommt eine besondere Bedeutung zu: Informationssicherheitsprozesse zahlen unmittelbar auf die Erfüllung von Datenschutzanforderungen ein, konkret auf die TOM. Der notwendige Schutz der Informationen (nicht nur der personenbezogenen Daten) erfordert Maßnahmen der Informationssicherheit, die im besten Fall als Informationssicherheits-Managementsystem organisiert sind, das angelehnt an den ISO 27001-Standard aufgebaut ist. Mit der Implementierung der Informationssicherheits-Maßnahmen werden bereits größtenteils die datenschutzrechtlichen TOM umgesetzt. Werden durch erfolgreiche Cyberattacken personenbezogene Daten entwendet (Data Breach), kommt es zu einem Datenschutzvorfall. In diesem Fall sind somit Informationssicherheit und Datenschutz gleichzeitig betroffen. ISMS und DSMS sollten deshalb harmonisiert sein. Je besser das Unternehmen in IT-/ Informationssicherheit aufgestellt ist, umso weniger müssen noch TOM speziell für Datenschutz ins Werk gesetzt werden; Informationssicherheit hebelt dann als Datensicherheit im besten Sinne den Datenschutz.



Quelle; 1 DSGVO (2018), *Artikel 32* | 2 ISO/IEC 27001 Standard (2013)

Abbildung 20: ISMS zahlt auf TOM und DSMS ein

Mit dieser Phase kann sich das Unternehmen als strategischer Vertrauenspartner für Kunden und Partner positionieren, hat es die langfristige Wettbewerbs- und Innovationsfähigkeit in der Datenökonomie abgesichert und den Grundstein für langfristige Kostensenkung durch die Harmonisierung sowie Interaktion von IT, Datensicherheit und Datenschutz gelegt. Eine Zertifizierung, durch die Etablierung des DSMS in der zweiten Phase vorbereitet, ist nun ein Muss, da Datenschutz Teil des strategischen Portfolios des Unternehmens ist.

4.2 Moderne IT-Architekturen automatisieren Datenschutz und Datensicherheit

Legacy strukturell bedingt in Datenökonomien von Nachteil

Viele Datenschutzpannen der letzten Jahre waren grundsätzlich nicht auf eine per se böswillige Ausnutzung von Kundendaten zurückzuführen, sondern auf für das Internetzeitalter inadäquate technische Maßnahmen wie fehlende Verschlüsselung oder fehlendes Hashing von Kennwörtern. Datenbanken mit sensiblen Daten befanden sich oft unzureichend oder gar nicht geschützt im Internet. Die mangelnde Berücksichtigung von sicherheitstechnischen Maßnahmen ist oft in der Historie der Systementwürfe zu finden, da in der Vergangenheit viele Systeme nicht für einen Anschluss an das Internet konzipiert wurden und somit ein vereinfachtes Setup ohne weitreichende Sicherheitsmerkmale verargumentiert werden konnte – auch wegen fehlendem regulatorischen und aufsichtlichen Druck.

Solche aus heutiger Sicht als Defizit einzuordnende Inadäquanz wird im Technologiemanagement als Technische Schulden bezeichnet. Technische Schulden lassen sich in IT-Architekturen ohne kontinuierliche Verbesserung der Systemlandschaft und ein Technologiemanagement prinzipiell nicht verhindern. Branchen, die IT schon verhältnismäßig lange einsetzen, sind daher von Technischen Schulden besonders betroffen: Datenbanken im öffentlichen Sektor, aber auch in Banken und Versicherungen anzutreffende Systementwürfe aus dem letzten Jahrhundert. Solche Systeme wurden immer wieder erweitert und mit zusätzlichen Funktionen ausgestattet, für die sie ursprünglich nicht ausgelegt waren; diese technologische Sedimentierung führt zu prinzipiell nur mit unverhältnismäßigem Aufwand weiterzuentwickelnden Systemen, deren Ertüchtigung für den Einsatz in öffentlich zugänglichen Netzen teuer, zeitaufwändig und komplex ist. Ein Neubau kann hier oft günstiger sein als eine Weiterentwicklung, denn die notwendigen Investitionskosten steigen proportional zum Alter der Systeme, da die alten IT-Architekturen nicht am technologischen Fortschritt partizipieren.

Moderne Technologie integriert Lösungsmuster für Datenschutz und Datensicherheit

Moderne Architekturansätze adressieren viele der Datenschutzanforderungen bereits implizit. Beispiele hierfür sind:

- Da bei Cloudtechnologie grundsätzlich nicht von einer Separation der Verarbeitungssphären auszugehen ist und die Infrastruktur prinzipiell von Dritten gesourct wird, müssen alle Module zugangs- und zugriffsgeschützt sein und alle Daten verschlüsselt
- Kubernetes als beispielhafte Basis vieler aktueller Systementwürfe verwaltet alle Aspekte der zugrundeliegenden Hardware: Festplatten, Netzwerk, CPUs, Arbeitsspeicher. Weil diese Ressourcen üblicherweise virtualisiert sind und dynamisch auf physische Hardware gemappt werden, ist eine durchgängige Verschlüsselung in mandantenfähigen Systemen prinzipiell notwendig (und um solche handelt es sich bei vielen Public Cloud Anbietern)

- Von nahezu durchgängig verfügbarer Hardwareverschlüsselung physischer Festplatten über eine zusätzliche Verschlüsselung der virtuellen Festplatten (wobei meistens sowohl providerverwaltete Schlüssel als auch Bring Your Own Key (BYOK) Szenarien umsetzbar sind) bis hin zu einer Datenbank- oder Feldverschlüsselung bieten moderne Systeme eine Vielzahl von Möglichkeiten der sicheren Datenspeicherung
- Selbiges gilt für den Netzwerkverkehr: von Security Komponenten wie Cillium zur Verschlüsselung von Netzwerkkommunikation auf OSI Layer 3 und/ oder 4 bis hin zu Service Meshes wie Istio zur Verschlüsselung auf dem Application Layer bieten sich vielfältige Optionen der Erhöhung der Sicherheit, die früher enormen Implementierungsaufwand nach sich zogen: Service Meshes sind in der Lage, transparente Punkt-zu-Punkt Authentifizierung einzelner Services mittels mTLS sicherzustellen und sämtliche Verbindungen auch transparent zu überwachen – ohne dass die Applikationen hierzu angepasst werden müssen. Viele Sicherheitsaspekte können so separat von der Business Logik und feingranular gesteuert werden, mit entsprechend niedrigerer Fehlerwahrscheinlichkeit in der Implementierung

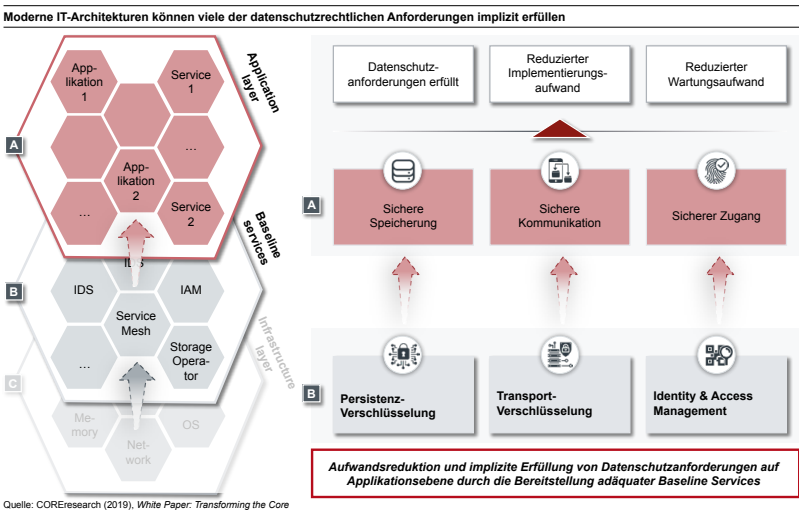


Abbildung 21: Moderne IT-Architekturen fördern Privacy-by-Design

Kurz zusammengefasst: moderne IT-Architekturentwürfe erlauben es Business Stakeholdern, Architekten und Entwicklern, sichere Systeme zu entwerfen ohne signifikante Budgets der Funktionsentwicklung aufwenden zu müssen und weil viele der Frameworks sich zu de facto Industriestandards entwickelt haben, kommen Verbesserungen einzelner Komponenten auch dem eigenen System zugute – ohne eigene Ressourcen dafür aufwenden zu müssen. Ein auf stetige Verbesserung ausgerichtetes Technologiemanagement kann durch moderne IT-Architekturen viele der datenschutzrechtlichen Anforderungen implizit erfüllen. Damit kann sich der Fokus auf das Business richten, Datenschutz und Datensicherheit werden durch einen modernen Tech Stack und im Hintergrund erfüllt.

4.3 Hinweise zur Praxis im Datenschutz

Technische Grundlagen für Datenschutz in der IT sind lange bekannt und bewährt

Für eine erfolgreiche praktische Umsetzung muss ein eingehendes Verständnis für wesentliche unterstützende Themen des Datenschutzes geschaffen werden. Deshalb werden hier die Themen Kryptographie, Pseudonymisierung/ Anonymisierung und Informationssicherheit erläutert. Diese Themen können in ihrer Bedeutung für den Datenschutz gar nicht überschätzt werden, bedürfen aus unserer Sicht jedoch der strukturierten Einordnung, um ihren praktischen Einsatz dem Einzelfall angemessen vorzunehmen.

4.3.1 Kryptographie für Datenschutz

Fünf kryptographische Primitive bilden das Rückgrat der Sicherheit im Internet

Die DSGVO ist das erste Datenschutzgesetz, das von „Verschlüsselung" als angemessene Sicherheitsmaßnahme für personenbezogene Daten spricht. Die Kryptographie bietet eine überschaubare Anzahl an Methoden, auf denen die komplette, auf das Internet aufbauende Wirtschaft fußt. In Abbildung 22 sind die kryptographischen Methoden über die Schutzziele Vertraulichkeit, Integrität, Authentizität und Nicht-Abstreitbarkeit aufgetragen. Das Hashen selbst ist kein Schutzziel an sich; da Hashes allerdings eine wichtige Rolle in der kryptographischen Kette spielen, müssen sie aufgeführt und im Folgenden auch in ihrer Verwendung im Datenschutz beschrieben werden.

Übersicht der kryptographischen Mittel – für Datenschutz relevant sind nur Vertraulichkeit und Hash

✓ Schutzziel gewährleistet ✓ Zuordnungsregel mindestens zwei Funktionen bekannt, De-Pseudonymisierung möglich

Methode \ Schutzziel	Vertraulichkeit			Integrität	Authen-tizität	Nicht-Abstreit-barkeit	Hash
	technisch	organis.	rechtlich				
Digitale Signatur				✓	✓	✓	
MAC (Message Authentication Code)				✓	✓		
Verschlüsselung symmetrisch	✓		✓	✓	✓		
Verschlüsselung asymmetrisch	✓		✓				
Hashen	✓[1]						✓
Pseudonymisierung (gem. DSGVO)		✓	✓				
Risikomindernde Pseudonymisierung		✓	✓				
Anonymisierende Pseudonymisierung	✓		✓				
Anonymisierung	✓		✓				

Quelle: COREresearch (2020) | 1 Wenn Urbild geheim

Abbildung 22: Kryptographische Primitive über Schutzziele

Verschlüsseln (Schutzziel Vertraulichkeit der Kommunikation und Speicherung) kann man symmetrisch (ein geheimer Schlüssel für Sender und Empfänger) und asymmetrisch (je ein Schlüsselpaar – privater und öffentlicher Schlüssel – für Sender und Empfänger). Die symmetrische Variante bietet neben dem Schutz der Vertraulichkeit auch den Schutz von Integrität (Unveränderbarkeit von Daten und Authentizität). Das Senden und Empfangen ist mit Speichern und Lesen gleichzusetzen. Deswegen kann Verschlüsslung auch als Datenschutzmaßnahme eingesetzt werden, um den leseberechtigten Kreis von Personen und Diensten auf personenbezogene oder besonders schützenswerte Daten wirksam zu beschränken, indem der geheime Schlüssel nur berechtigten Personen und Diensten zugänglich gemacht wird. Vorbehaltlich der sicheren Verwahrung der Schlüssel, zum Beispiel mittels Hardware Security Modul (HSM), kann ein unberechtigter Zugriff sicher ausgeschlossen werden.

Will man mit der asymmetrischen Verschlüsselung die beiden letztgenannten Schutzziele umsetzen, geht man zur digitalen Signatur über: diese bietet als einzige kryptographische Methode auch das Schutzziel Nicht-Abstreitbarkeit, d.h., dass der Sender einer digital signierten Nachricht seine Urheberschaft dieser Nachricht nicht abstreiten kann. Während die Digitale Signatur auf asymmetrische Kryptographie baut, nutzt ein MAC (Message Authentication Code) symmetrische Kryptographie und schützt Integrität und Authentizität, aber nicht die Nicht-Abstreitbarkeit, da der verwendete geheime Schlüssel mindestens zwei Kommunikationspartnern bekannt sein muss, somit nicht eine einzige Person als Urheber der Nachricht in Frage kommt.

Hashen ist für Nutzung im Datenschutz überschätzt

Mit diesen vier Methoden werden alle klassischen Schutzziele umgesetzt. In der IT-Sicherheit spielen noch Hashverfahren eine große Rolle. Hashfunktionen sind Einwegfunktionen, welche eine große Datenmenge (das „Urbild“) auf eine kleine Datenmenge abbilden, ohne von dieser kleinen Datenmenge auf das Urbild schließen zu können. In der Praxis werden beliebig große Daten auf 160-512 Bit große, Hashes genannte Datenblöcke abgebildet. Meistens werden heute sogenannte kryptographische Hashfunktionen verwendet, welche kollisionsresistent sind und keine Möglichkeit bieten das Urbild zu errechnen. Gleichwohl wird dasselbe Urbild immer auf genau denselben Hash abgebildet, wodurch der Hash zu einem „Fingerabdruck“ (engl. Fingerprint) des Urbildes wird.

Obwohl mathematisch möglich, werden Hashes nicht für die Gewährung von Vertraulichkeit verwendet. Die Hauptfunktion eines Hash ist die Integritätsprüfung des Urbildes. Die zweite Funktion ist die Signierung des Hash zum Beweis der Urheberschaft (Authentizität) eines Urbilds. Weiterhin werden Hashfunktionen zum Speichern von Passwörtern genutzt. Dabei wird nicht das Passwort selbst gespeichert, sondern nur sein Hash, wodurch ein Angreifer das ursprüngliche Passwort nicht erraten kann, selbst wenn er Zugriff auf den Hash erlangt. Ende 2018 musste die Chatplattform Knuddels ein Bußgeld in Höhe von EUR 20.000 zahlen[20], weil sie Passwörter im Klartext gespeichert hatte, welche bei einem Angriff entwendet wurden. Für einen effektiven Datenschutz muss das Passwort vor dem Hashen um einen zufälligen Salt ergänzt werden, um die Schwierigkeit für einen Angreifer zu erhöhen.

Die besonderen Verwendungszwecke im Datenschutz liegen in der differentiellen Privatsphäre und in der Pseudonymisierung (Kapitel 4.3.2). Hashen zum Zwecke der Pseudonymisierung ist nur dann sinnvoll, wenn die Varianz des Inputs groß ist. Das entspricht technisch der gleichen Anforderung wie der eines guten Passwortes, dieses darf nicht zu kurz sein. Mit mindestens 10, besser 16 alphanumerischen Zeichen ist man auf der sicheren Seite. Insofern macht im Datenschutz das Hashen von Postleitzahlen, Geburtstagen oder auch Straßennamen zur Pseudonymisierung keinen Sinn, denn ein Angreifer kann in kurzer Zeit alle in Frage kommenden Hashes selbst berechnen und mit dem gesuchten Hash vergleichen.

[20] Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg (2018), 03.05.2020

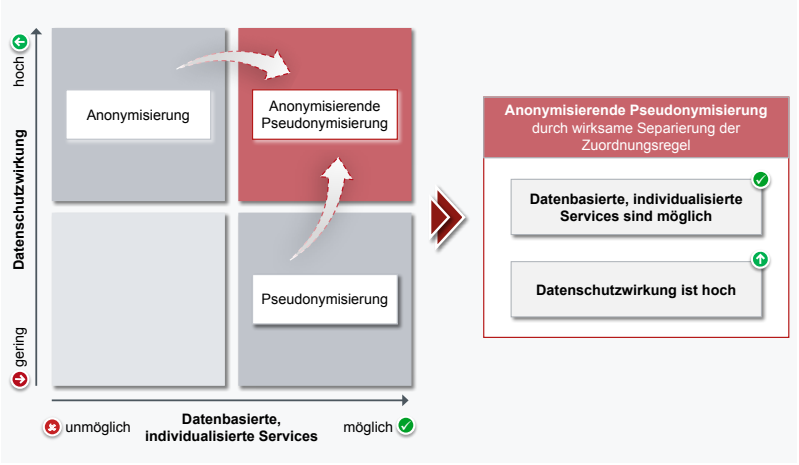
4.3.2 Pseudonymisierung und Anonymisierung

Pseudonymisierung hat das größte Potenzial, Datenschutz zu hebeln – wenn Gesetzgeber und Aufsicht klug novellieren

Pseudonymisierung ist ein noch recht unbeschriebenes Blatt im praktischen Datenschutz, d.h. im Umkehrschluss kann die Pseudonymisierung noch eine große Zukunft im Datenschutz entfalten. Die DSGVO unterscheidet bei der „Hinzuziehung zusätzlicher Informationen“ (die Zuordnungsregel) nicht zwischen den verschiedenen technischen, organisatorischen und rechtlichen Möglichkeiten der Aufbewahrung der Zuordnungsregel. Diese kann beim Verantwortlichen verbleiben, der sowohl die Pseudonymisierung vorgenommen hat als auch die pseudonymisierten Daten verarbeitet. Sie kann aber auch in einer anderen Abteilung des gleichen Unternehmens aufbewahrt werden oder bei einem Externen mit oder ohne Notarfunktion. Schlussendlich kann die Zuordnungsregel sogar rechtlich und technisch sicher gelöscht und so eine Anonymisierung erreicht werden. Die drei Funktionen der Pseudonymisierung können somit durch einen Verantwortlichen ausgeführt oder auf zwei oder drei Verantwortliche aufgeteilt werden:[21]

- Verantwortlicher 1 (V1) führt die Pseudonymisierung durch
- Verantwortlicher 2 (V2) bewahrt die Zuordnungsregel auf
- Verantwortlicher 3 (V3) verarbeitet die pseudonymisierten Daten

Anonymisierende Pseudonymisierung als Lösung für individualisierte Services mit gutem Datenschutzniveau



Quelle: COREresearch (2020)

Abbildung 23: Funktionstrennung der Verantwortlichen bei der Pseudonymisierung

Sind alle drei Rollen bei einem Verantwortlichen vereinigt, ist die Schutzwirkung der Pseudonymisierung gering, da die Daten zwar nicht personenbezogen verarbeitet werden, aber jederzeit zugeordnet werden können. Das gilt auch, wenn Rollen der Verantwortlichen innerhalb einer Organisation zum Beispiel auf verschiedene Abteilungen aufgeteilt sind. Ist allerdings rechtlich (z.B. in einer ersten DSGVO-Novelle) und vertraglich sichergestellt, dass V2 ein Notar und die Zuordnungsregel in seinem Machtbereich sicher vor dem Zugriff durch V1 und V3 ist, wird für die zwei Kombinationsmöglichkeiten des separierten V2 eine anonymisierende Pseudonymisierung erreicht. Diese bietet eine der Anonymisierung vergleichbar hohe Schutzwirkung, bewahrt aber die Möglichkeit der Pseudonymisierung bis hin zur De-Pseudonymisierung der Daten.

[21] Roßnagel (2018).

Anonymisierende Pseudonymisierung als neuer praxisrelevanter Lösungsbaustein

Wird die Zuordnungsregel gelöscht, sind die Daten anonymisiert. Die Funktionstrennung auf drei Verantwortliche V1, V2 und V3 bietet ein Ausdifferenzieren der Anwendungsmöglichkeiten personenbezogener Daten in drei Qualitätsstufen der Pseudonymisierung. Hier bleibt es spannend zu sehen, welche Geschäftsfelder sich aus diesem Möglichkeitsraum ergeben.

Eine große Herausforderung bei der Pseudonymisierung ist, dass sich Datensätze nicht nur über einen eindeutigen Identifier oder direkt personenbezogenen Attributen einer Person zugeordnet werden können, sondern dass auch eine eindeutige Kombination von Attributen, welche einzeln nicht für eine Identifizierung herangezogen werden können, dazu genutzt werden können, einen eindeutigen Personenbezug herzustellen. So können mit der Kombination von Postleitzahl, Geburtsdatum und Geschlecht 87% aller US-Amerikaner eindeutig identifiziert werden.[21] Eine solche Kombination von Attributen wird als Quasi-Identifier bezeichnet. Durch verschiedene Generalisierungsverfahren kann das Entstehen von Quasi-Identifiern vermieden werden. Zu den wichtigsten Generalisierungsverfahren gehören k-anonymity, l-diversity und t-closeness, welche für einen effektiven Schutz von pseudonymisierten Daten immer angewandt werden müssen. Neben der Generalisierung kann auch eine Randomisierung der Daten mittels Permutation oder dem Hinzufügen von Rauschen erfolgen.

Die differentielle Privatsphäre bietet mit der Pseudonymisierung weitere Öffnungsklausel für datengetriebene Wirtschaft

Eine interessante Forschungsrichtung im Bereich der randomisierenden Anonymisierungstechniken ist die differentielle Privatsphäre (DP). Mit Hilfe von DP-Algorithmen werden aus vielen personenbezogenen Datensätzen Aggregate gebildet, die abhängig von der Konfiguration der Algorithmenparameter verschiedene Qualitätsstufen der Anonymisierung erreichen. Differentielle Privatsphäre lässt keine Rückschlüsse auf ein bestimmtes Individuum zu, die personenbezogenen Daten werden randomisiert. Man erhält aber gesuchte Informationen zu einer Menge von Personen. Diese aggregierten Daten dürfen nach Erwägungsgrund 162 DSGVO für statistische Zwecke, wie zum Beispiel zu Forschungszwecken verwendet werden.

Jedoch dürfen die Ergebnisse der Verarbeitung in Form einer statistischen Analyse nicht für Entscheidungen oder Maßnahmen gegenüber einzelnen natürlichen Personen zur Anwendung kommen. Im Unterschied zur Anonymisierung einzelner Datensätze, die ggf. durch bestimmte Korrelationen der enthaltenen Informationen und/ oder Hinzuziehung von Informationen externer Quellen de-anonymisiert werden, können DP-Aggregate nicht de-anonymisiert werden. Diese Eigenschaft der differentiellen Privatsphäre wird durch drei aufeinanderfolgende mathematische Methoden erreicht:

- Hashing: Verschleierung der ursprünglichen Daten
- Subsampling: Beschränkung der Daten auf eine Teilmenge des Originals
- Noise Injection: Anreicherung mit Zufallswerten (Rauschen)

Die differentielle Privatsphäre öffnet den Weg für neue kommerzielle und gleichzeitig datenschutzkonforme Dienste zum Beispiel zu Datenanalysen für ein verbessertes Marketing – wie erfolgreich von Apple und Google eingesetzt.

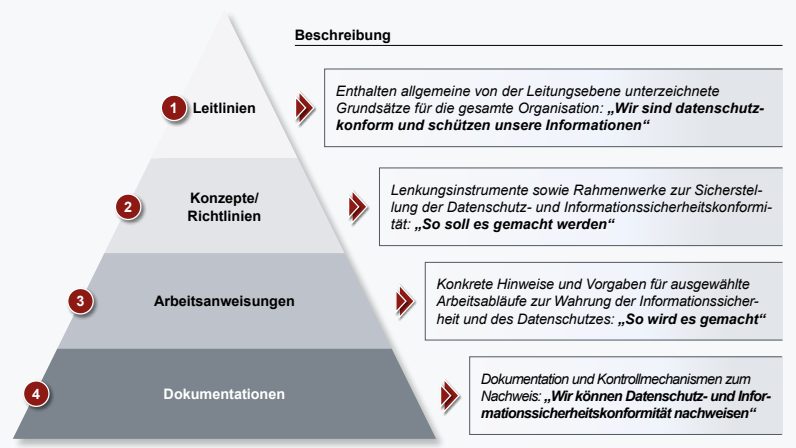
[21] Sweeney, Latanya (2000).

4.3.3 Informationssicherheit

Informationssicherheit als Voraussetzung für Datenschutz/ Datensicherheit

Datenschutz und Informationssicherheit sind nicht zu trennende zwei Seiten der gleichen Medaille. Beide Seiten sind über Artikel 32 „Sicherheit der Verarbeitung“, Artikel 25 DSGVO „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ sowie § 64 BDSG „Anforderungen an die Sicherheit der Datenverarbeitung“ in der technisch-organisatorischen Ausgestaltung verbunden. Ein ISMS besteht aus Policies und Prozessen, hier im Beispiel (Abbildung 24) in vier Ebenen organisiert:

Vier Ebenen eines Informationssicherheits-Managementsystems (ISMS)



Quelle: COREresearch (2020)

Abbildung 24: Informationssicherheits-Managementsystem umfasst vier Ebenen

Informationssicherheit umgesetzt in einem ISMS gewährleistet Datensicherheit und dient als Modell für das DSMS in organisatorischer, technischer, rechtlicher und personeller Aufstellung. Im „ISMS nach ISO 27001 – Blaupause für den Einsatz in Unternehmen“-Blogpost wird die detaillierte Wirkungsweise eines ISMS als Werkzeug zur Datenschutzkonformität vorgestellt und es werden Hinweise zum Aufbau eines zertifizierungsfähigen ISMS gemäß ISO 27001 gegeben.

https://core.se/de/techmonitor/isms-nach-iso-27001

5 Fazit

Vertrauen ist essenziell für erfolgreiches Wirtschaften; Datenschutz begründet Vertrauensbildung

Datenschutz und Vertrauen gemeinsam dienen als Rohstoff einer erfolgreichen Digitalwirtschaft. Die technologische Entwicklung bedeutet immer sowohl Chancen als auch Risiken. Der Gesetzgeber adressiert mit modernen Datenschutzgesetzen wie der europäischen DSGVO die Risiken, welche sich für Endverbraucher ergeben; gleichzeitig sehen die Autoren des vorliegenden Papiers deutliche Chancenpotenziale in der aktiven, technologiebasierten Gestaltung der Erfüllung der gesetzlichen Vorgaben, was auch seitens des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), Herrn Professor Ulrich Kelber, ähnlich gesehen wird. Ihm zufolge „ist Datenschutz ein Grundrechtsschutz, den es zu wahren gilt." und konkretisiert „Profiling und Tracking sind nicht modern, moderne Digitalisierung geht auch ohne Bespitzelung, das informationelle Vertrauen wird zur zentralen Frage."[22]

Die DSGVO findet weltweit viele Nachahmer und selbst im zweifelsohne technologiefreundlichen Kalifornien wurde die europäische Gesetzgebung in Form des California Consumer Privacy Act adaptiert – dies geschieht mit Sicherheit nicht gegen die Interessen der dort ansässigen global agierenden Technologiekonzerne.

Europa als Vorteil beim Aufbau datenbasierter Geschäftsmodelle mit inhärentem Datenschutz

Es besteht realistisch betrachtet keine Option mehr, Datenschutz in der Unternehmenssteuerung zu negieren, da der Sanktionsdruck für alle Wirtschaftsbereiche steigt, aktuelle Geschäftsmodelle ggf. im Risiko stehen oder auch neue, innovative auf Daten basierende Angebote ohne adäquaten Datenschutz nicht im Markt positioniert werden können. Einige Marktteilnehmer, wie z.B. die großen Plattformanbieter haben dies bereits verinnerlicht und ihre Geschäftsstrategien entsprechend angepasst. Europäische Unternehmen sollten – aus Sicht der Verfasser – die Vorteile der Rahmenbedingungen im Wettbewerb mit den westlichen oder auch asiatisch geprägten Konkurrenten als Chance begreifen. Europa kann immer noch Vorreiter der datengetriebenen, auf Freiwilligkeit, Transparenz und Sicherheit bauenden Wirtschaft werden. Diese Ökonomie ist nicht aufzuhalten, gestalten sollten wir sie maßgeblich.

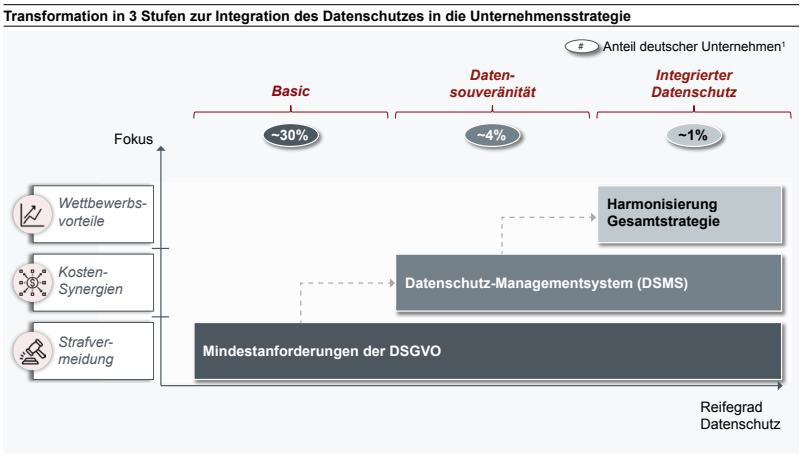


Abbildung 25: 3-Stufen-Modell für nachhaltigen Datenschutz

[22] Prof. Ulrich Kelber (2020), 26.–27.02.2020.

Wenn Datenschutz von Unternehmen als Grundlage für eine Vertrauensbildung seitens der Kunden verstanden und integraler Bestandteil der Unternehmensstrategie werden soll, dann kann dies mit einem 3-Stufen-Modell effektiv und effizient erreicht werden.

- Die Basisstufe 1 stellt basierend auf wenigen wesentlichen Hebeln abgeleitet aus der Praxis die Erfüllung der gesetzlichen Mindestanforderungen sicher
- Auf Stufe 2 wird der souveräne Umgang mit Datenschutz zur Gestaltung von Vertrauensnetzwerken mit Hilfe eines umfassenden Datenschutz-Managementsystems (DSMS) realisiert, welches zukünftig auch eine externe Zertifizierung und ein unabhängiges Gütesiegel erhalten kann
- Die dritte Stufe einer weitreichenden Gestaltung von Datenschutz positioniert diesen als gleichberechtigten Bestandteil der Unternehmensstrategie neben der Geschäfts- und IT-Strategie

Die Nutzung moderner IT-Architekturen ermöglicht die Schaffung hochqualitativer wie auch effizienter Lösungen auf allen Stufen der Gestaltung von Datenschutz und Datensicherheit.

Perspektive wechseln: Datenschutz nutzen

Abschließend möchten wir Verfasser zur Bündelung der Kräfte aufrufen. Aus dem Gegeneinander von Datenschützern und Datenverwertern und dem gegenseitigen Beäugen von Gesetzgeber und der Wirtschaft muss eine Kooperation zum Wohle des Kundennutzens und damit des wirtschaftlichen Erfolgs werden. Datenschutz ist nicht notwendiges Übel, sondern eröffnet aktiv die Chance für Vertrauensbildung von Kunden in Produkte und Services der Digitalwirtschaft. Dieses Vertrauen von Kunden als Grundlage für nachhaltig erfolgreiches Wirtschaften ist der wertvolle Rohstoff, der gesichert werden muss.

Quellen

Alexander Roßnagel (2018): *Pseudonymisierung personenbezogener Daten – Ein zentrales Instrument im Datenschutz nach der DSGVO*, ZD 2018, 243.

Accessnow (2019): *One year under the EU GDPR*

Bitkom (2019): *DSGVO, ePrivacy, Brexit– Datenschutz und die Wirtschaft*

Bitkom (2019): *Angriffsziel deutsche Wirtschaft: mehr als 100 Milliarden Euro Schaden pro Jahr*

Bitkom (2019): *Nutzervertrauen in Datensicherheit im Internet steigt*

Bundesministerium der Justiz und für Verbraucherschutz (2007): *Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 11 des Gesetzes vom 11. Juli2019 (BGBl. I S. 1066) geändert worden ist*

Bundesverband Deutscher Zeitungsverleger e.V. (2019): *Infotag Datenschutz 05.12.2019*

BVDW (2019): *BVDW-Mitgliederumfrage zur EU-Datenschutzgrundverordnung (DSGVO)*

Cisco (2019): *Data Privacy Benchmark Study*

CMS (2020): *GDPR Enforcement Tracker,* abgerufen am 24.04.2020

COREresearch (2015): *White Paper: Wollen » Können*

COREresearch (2019): *White Paper: Transforming the Core*

Der Europäische Datenschutzbeauftragte (2020): *Entwicklungsgeschichte der Datenschutz-Grundverordnung*

Die Welt (2018): *So teuer sind Hackerangriffe für Unternehmen,* abgerufen am 18.05.2020

Digital Analytics (2019): *Trendstudie 2019*

Europäische Kommission (2017): *Vorschlag für eine Verordnung des europäischen Parlaments und des Rates*

European Commission (2016): *Article 29 Data Protection Working Party*

European Data Protection Board (2019): *Report on the implementation of GDPR*

FAZ (2019): *Die wichtigste Ressource für Tech-Unternehmen,* abgerufen am 01.05.2020

Geldinstitute (2020): *Millionenschäden: Die Kosten eines Datenlecks*

Handelsblatt (2019): *Grafiken des Monats – 8. August 2019*

Heise online (2019): Bundestag: *Deutlich mehr Stellen für die Bundesdatenschutzbehörde,* abgerufen am 15.05.2020

IDC (2018): *The Digitization of the World*

IDC (2019): *Industrieunternehmen auf dem Wen in das datenbasierte Tagesgeschäft*

IDW (2019): *Datenmenge explodiert*

IDW (2020): *Datenschutz: Ungeliebtes Regelwerk*

Ipsos (2019): *Internet Security & Trust*

Irish Data Protection Commission (2020): *Annual Report 2019*

ISO/IEC 27001 Standard (2013)

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg (2018): *LfDI Baden-Württemberg verhängt sein erstes Bußgeld in Deutschland nach der DSGVO*, abgerufen am 03.05.2020

Prof. Ulrich Kelber (2020): *Anlässlich der Fachveranstaltung „13. Praxistage Datenschutz“,* 26.–27.02.2020, Köln

Reguvis (Bundesanzeiger Verlag) (2019): *Digital Dialog Insights 2019*

Sweeney, Latanya (2000): *Simple Demographics Often Identify People Uniquely (Datenschutz Working paper 3)*

Thomson Reuters (2019): Survey, GDPR+1 YEAR

TrustArc (2018): GDPR Compliance Status

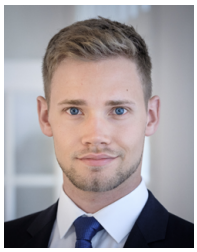
Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) in der aktuellen Version des ABl. L 119, 04.05.2016

YouTube (2019): *Werbevideo von Apple: Privacy on iPhone—Simple as that—Apple,* abgerufen am 03.05.2020

Autoren

Magdalena Buski ist Transformation Fellow bei CORE. Sie absolvierte einen Bachelor of Arts in Betriebswirtschaftslehre an der HTWK in Leipzig. Ihre Schwerpunkte bei CORE sind die strategische Konzeptionierung und Umsetzung von IT-Transformationen und der Aufbau von Informationssicherheits-Managementsystemen nach ISO 27001.

Magdalena Buski
magdalena.buski@core.se



Marc-André Dymala ist Transformation Manager bei CORE. Er hält zwei Masterabschlüsse, einen in International Business Management (SWUFE Chengdu, China) und einen in Chinese European Economics and Business Studies (HWR Berlin). Seine Schwerpunktthemen umfassen digitale Transformationen sowie ISMS (ISO 27001) und Datenschutz.

Marc-André Dymala
marc-andre.dymala@core.se

Waldemar Grudzien ist Expert Director bei CORE. Er wurde in Elektrotechnik promoviert und verfügt über ein Diplom in VWL. Schwerpunkte seiner Arbeit sind Informationssicherheit und Datenschutz – in Theorie und Praxis, inklusive operationeller Tätigkeiten als ISB und DSB in verschiedenen Klientenstrukturen.

Dr. Waldemar Grudzien
waldemar.grudzien@core.se

Autorenteam

Christian Böhning ist Managing Director bei CORE. Er besitzt langjährige Erfahrung in der Durchführung digitaler Transformationsvorhaben in durch IT nachhaltig veränderten Branchen. Schwerpunkt seiner Arbeit sind Programme zur IT-Architekturmodernisierung, Durchführung von Compliance-Initiativen und Neuausrichtung von IT-Organisationen.

Christian Böhning
christian.boehning@core.se

Johannes von Bonin ist Transformation Associate bei CORE. Seinen Masterabschluss in Economics of the Middle East absolvierte er an der Universität Marburg und der Lebanese American University in Beirut. Bei CORE arbeitet er in den Bereichen digitale Transformation, agiles Projekt- und Produktmanagement und Datenschutz.

Johannes von Bonin
johannes.bonin@core.se

Nadine Hofmann ist Transformation Associate bei CORE. Sie studierte Luft- und Raumfahrttechnik in Braunschweig und Dresden. Ihre Beratungskompetenz fokussiert sich auf technischen Datenschutz und Informationssicherheit (Schwerpunkte IAM und Security Operations Center). Sie unterstützt Klienten beim Aufbau von Managementsystemen.

Nadine Hofmann
nadine.hofmann@core.se

Über COREresearch

Als unabhängiger Technologie Think Tank erforschen wir die Systematik technologisch getriebener Transformationen in Industrien mit einem hohen Anteil an IT im Wertschöpfungsprozess. Im Rahmen unserer Forschungsaktivitäten analysieren wir Märkte und Technologien, thematisieren Strukturen, Ursachen und Wirkmechanismen des technologischen Wandels und kuratieren Ergebnisse für Klienten und die Öffentlichkeit. Darüber hinaus stellen wir ausgewählte Resultate unserer interdisziplinären Forschungen im Rahmen von übergreifenden Publikationen, Einzelstudien sowie Vorträgen einer breiteren Öffentlichkeit zur Verfügung.

https://core.se/de/publications/white-paper

Disclaimer

CORE SE
Am Sandwerder 21–23
14109 Berlin
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Am Sandwerder 21–23
14109 Berlin
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Limmatquai 1
8001 Zürich
https://core.se/
Phone: +41 44 261 0143
office@core.se

COREtransform Ltd.
Canary Wharf, One Canada Square
London E14 5DY
https://core.se/
Phone: +44 20 328 563 61
office@core.se

COREtransform Consulting MEA Ltd.
DIFC – 105, Currency House, Tower 1
P.O. Box 506656
Dubai I VAE
https://core.se/
Phone: +97 14 323 0633
office@core.se