Foto: © arahan

WAS SIE **WISSEN SOLLTEN**

Die EU vereinheitlich das Datenschutzrecht, so dass europaweit tätige Unternehmen ab 2018 anstelle eines Flickenteppichs nationaler Datenschutzgesetze nur noch ein Datenschutzgesetz, die „Datenschutz-Grundverordnung" (DS-GVO) einhalten müssen. Ausgewählte Änderungen, die insbesondere für Dienstleister aus den Bereichen Marketing, Kundenkommunikation und Call Center von Bedeutung sind, stehen im Mittelpunkt dieses Beitrags.

Im Dezember 2015 wurde die Einigung zur Neuregelung des europäischen Datenschutzrechts erzielt. Mit der Veröffentlichung der Datenschutz-Grundverordnung (DS-GVO) und ihrem Inkrafttreten wird Ende des zweiten Quartals 2016 gerechnet. Anschließend haben die betroffenen Unternehmen zwei Jahre Zeit, ihre Organisation, Prozesse und Verarbeitungen an die neuen Regelungen anzupassen, bis die DS-GVO dann das bestehende Datenschutzrecht in der EU ersetzt. Dabei ergibt sich für alle Unternehmen und deren Dienstleister eine neue Rechtssituation, die insbesondere durch neue Pflichten, aber auch durch neue Haftungs- und Bußgeldregelungen geprägt ist. Dabei bemisst sich der Bußgeldrahmen auf bis zu 20 Mio. Euro und mehr. (siehe Tabelle 1). Das deutsche Datenschutzgesetz, das „Bundesdaten-

TABELLE 1 Eckdaten zur DS-GVO

Finale Beschlussfassung	Durch EU-Rat und EU-Parlament voraussichtlich im Sommer 2016
Inkrafttreten	20 Tage nach Verkündung im EU-Amtsblatt
Wirksamwerden	2 Jahre nach Inkrafttreten (Übergangszeit)
Übergangszeit	Das bisherige Recht wird weiter angewendet.
Unmittelbare Gültigkeit	Das Gesetz gilt unmittelbar, das heißt, es wird keine nationale Umsetzung mehr geben. Lediglich in wenigen Ausnahmen darf beziehungsweisemuss der deutsche Gesetzgeber eigene Gesetze erlassen.
Ende des Bundesdatenschutzgesetzes (BDSG) Inhaltliche Änderungen	Das BDSG wird mit dem Ablauf der Übergangszeit ungültig. Der Text ist final. Die redaktionelle Überarbeitung sowie die Übersetzung in die Nationalsprachen stehen aus.
Betroffene Organisationen	Unternehmen, Verbände, Vereine, Parteien, Behörden, Ministerien usw.

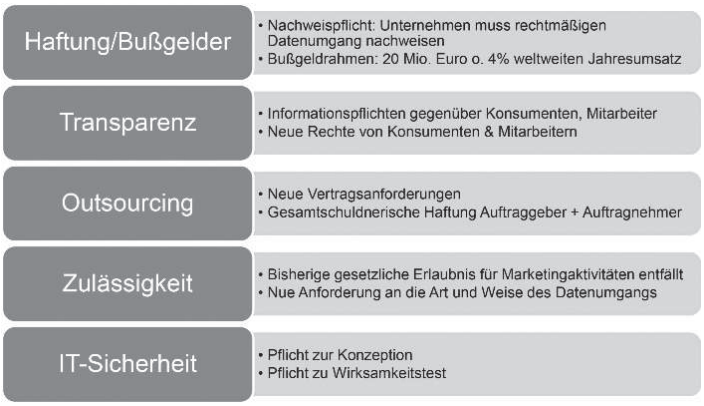

Abb. 1: Ausgewählte Änderungen.

schutzgesetz“ (BDSG), verliert dann seine Gültigkeit.

Die DS-GVO verändert die Rechtslage im Datenschutz weitreichend, da sie keinen Bereich verschont (siehe Abbildung „Ausgewählte Änderungen“). Besonders markant ist insbesondere im Bereich der Datenschutzorganisation die Abkehr von der Unschuldsvermutung hin zu einer Schuldvermutung.

Unternehmen müssen zukünftig belegen können, dass sie die Vorschriften der DS-GVO einhalten.

Hohe Bußgelder

Damit entfällt für die Datenschutzaufsichtsbehörden die Notwendigkeit, ein Verschulden zu ermitteln. Sie können sich auf die Prüfung des „Unschuldsbeweises“ beschränken. Gelingt dieser nicht, drohen Bußgelder von bis zu 10 Mill. Euro oder – sofern höher – zwei Prozent des weltweiten Jahresumsatzes. Für ausgewählte Verstöße, wie zum Beispiel eine nicht fristgerechte Reaktion bei Beschwerden oder unterlassene Informationen von betroffenen Personen, verdoppelt sich der Bußgeldrahmen auf bis zu 20 Mio. Euro oder – sofern höher – vier Prozent des weltweiten Jahresumsatzes. Es lohnt sich deshalb, frühzeitig die Anforderungen der DS-GVO mit Blick auf das eigene Unternehmen zu analysieren und die notwendigen Anpassungen vorzunehmen (siehe Abb. 1).

1. Beweise Deine Unschuld!

Die Nachweispflicht bedeutet, dass für alle Vorschriften der DS-GVO zukünftig Belege vorhanden sein müssen, wie diese eingehalten werden. Faktisch gibt es keine Vorschrift mehr, deren Verletzung nicht bußgeldbewehrt ist. Ein unternehmensweites aktuell gehaltenes Dokumentationssystem bietet sich für die Umsetzung an. Dieses sollte unter anderem folgende Darstellungen umfassen:

- Datenschutzkonzept,
- IT-Sicherheitskonzept,
- Beschreibung aller Prozesse, die personenbezogene Daten verarbeiten,
- Arbeitsanweisung zum Umgang mit personenbezogenen Daten,
- Darstellung der rechtlichen Zulässigkeit der Datenverarbeitung pro Datum sowie Löschfrist pro Datum.

Um eine entlastende Wirkung zu entfalten, müssen die Dokumente und Beschreibungen aktuell sein. Änderungen in Prozessen, Softwaresystemen, aber auch Werbe- und Marketingmaßnahmen bedürfen grundsätzlich sowohl einer Prüfung auf ihre rechtliche Zulässigkeit als auch die Anpassung der Dokumentation.

Beispiel: Kundendaten sollen segmentiert werden. Es muss geprüft werden, ob es eine Vorschrift in der DS-GVO gibt, die eine solche Segmentierung erlaubt. Anschließend müssen alle betroffenen Kunden per E-Mail oder Brief informiert werden, dass ihre Daten für einen neuen Zweck verarbeitet werden (siehe Abschnitt 2).

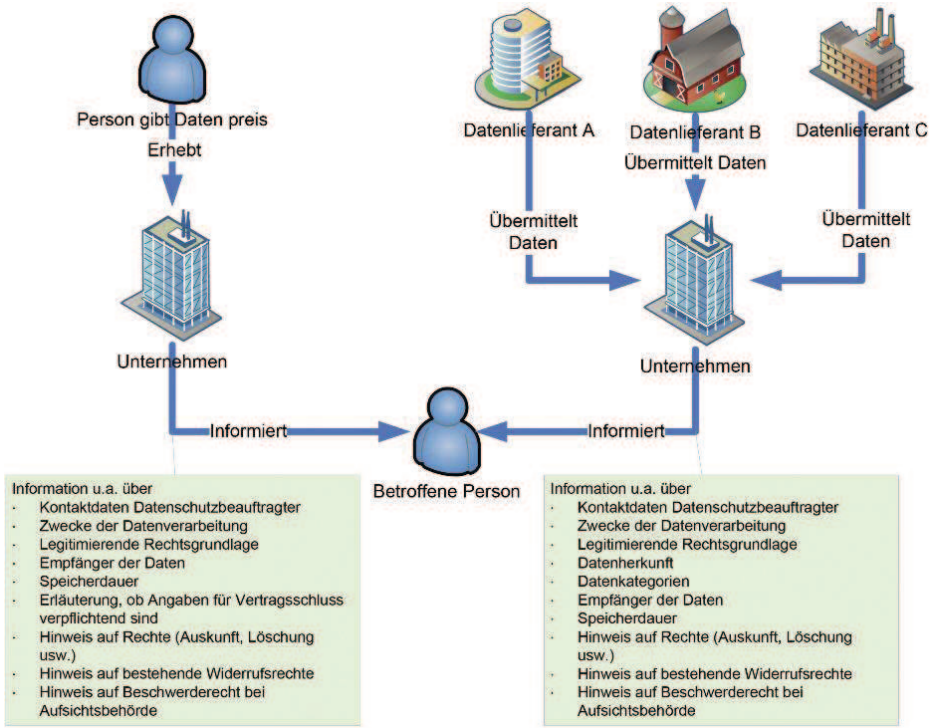

Abb. 2: Überblick über Informationspflichten gegenüber betroffenen Personen.

2. Neue Informationspflichten

Transparenz gegenüber Kunden, Mitarbeitern und anderen Personen, deren Daten verarbeitet werden, ist ein weiterer Eckpfeiler der DS-GVO. Dazu müssen Unternehmen zukünftig Personen, deren Daten verarbeitet werden, umfangreicher als bisher informieren. Die Informationspflicht gilt sowohl bei einer Erhebung bei oder mit der betroffenen Person wie auch bei einer Erhebung bei Dritten, wie etwa im Rahmen von Bonitätsprüfungen oder auch bei Entnahmen von Ansprechpartnern aus Firmenwebseiten. Die Informationspflicht entfällt, wenn die betroffene Person über alle Angaben bereits Kenntnis hat. Dieses bleibt durch die Vielzahl der zu machenden Angaben eher die Ausnahme (siehe Abb. 2). Im Outsourcing liegt die Verantwortung bei den Auftraggebern.

Werden die Daten für neue Zwecke verarbeitet, müssen alle betroffenen Personen erneut informiert werden.

Die Information kann per E-Mail oder auch per Brief gegeben werden. Es bietet sich beispielsweise an, Verträgen diesbezügliche Informationsblätter beizulegen. Ein „Verstecken“ in den AGB oder in einer Datenschutzerklärung auf der Webseite dürfte eher nicht ausreichend sein.

Da Verbraucher zukünftig immer wieder insbesondere auf Ihre Beschwerderechte hingewiesen werden müssen, könnte die Bereitschaft zunehmen, sich über mutmaßliche Datenschutzverstöße bei der Aufsichtsbehörde zu beschweren. Heute kennen viele Verbraucher dieses Beschwerderecht nicht. Der Rechtsfertigungsdruck gegenüber Verbrauchern und der Datenschutzaufsicht steigt weiter und sorgt für zusätzliche Herausforderungen in der Kundenkommunikation.

3. Änderungen beim Outsourcing

Die Einschaltung von Dienstleistern zum Beispiel im Rahmen des Outsourcings gestaltet sich für die Auftraggeber weiter nach weitgehend bekannten Regeln. Gleichwohl werden die Anforderungen geschärft und stärker in die Bußgeldandrohung einbezogen. Dies reicht von der Maßgabe zum Einsatz nur solcher Auftragsverarbeiter, die hinreichende technische und organisatorische Maßnahmen garantieren können über die Verpflichtung zur Einbeziehung der Sicherheitskonzepte der Dienstleister in eine eventuell durchzuführende Datenschutzfolgenabschätzung bis zur Vergabe eines Auftrags nur in Form eines schriftlich oder in elektronischer Form abgeschlossenen Vertrages mit den gesetzlich vorgegebenen Inhalten.

Dagegen kommt es im Hinblick auf den Dienstleister, Auftragsverarbeiter genannt, zu einem regelrechten Paradigmenwechsel: Der Auftragsverarbeiter wird jetzt selber Normadressat. Dies gilt nicht nur für die Kernnorm der Auftragsverarbeitung sondern auch für viele weitere Normen, in denen seine Verantwortlichkeit ausdrücklich genannt wird. Hervorzuheben ist dabei seine gesamtschuldnerische Haftung mit dem Auftraggeber sowie die Bußgeldbewehrung insbesondere bei Verstoß gegen Regelungen zur Auftragsverarbeitung, wie beispielsweise die Auftragsdurchführung ohne schriftlichen Vertrag, ohne dokumentierte Weisungen oder den Einsatz von Unterauftragnehmern ohne (dokumentierte) Zustimmung der Auftraggeber.

Zudem gilt der Auftragsverarbeiter, der ohne oder entgegen einer Weisung oder einen Vertrag arbeitet, selbst als „für die Verarbeitung Verantwortlicher“. Das wirkt sich insbesondere im Bereich der Bußgeldtatbestände aus, da sich der Auftragsverarbeiter in diesen Fällen regelmäßig nicht auf eine eigene Rechtsgrundlage berufen kann und damit unzulässiger Weise personenbezogene Daten verarbeitet.

Auftraggeber wie Auftragsverarbeiter müssen bestehende Dienstleistungsverhältnisse daraufhin überprüfen, ob sie den neuen Anforderungen gerecht werden. Soweit dies nicht der Fall ist, zum Beispiel weil entsprechende Verträge fehlen, ist dies bis zur Geltung der DS-GVO in 2018 zu heilen, da sie sonst in ein erhebliches Bußgeldrisiko laufen.

Die Dokumentation zum Nachweis der ordnungsgemäßen Auftragsabwicklung kann zum Beispiel anhand des GDD/BvD Standard „Anforderungen an Auftragnehmer

nach § 11 BDSG“ – Datenschutzstandard DS-BvD-GDD-01 erstellt beziehungsweise überprüft werden.

4. Zulässigkeit von Marketing und Werbeaktionen

Die bisher in Deutschland gültigen speziellen Regelungen im Bundesdatenschutzgesetz (BDSG) zur Verarbeitung personenbezogener Daten für Marketing- und Werbezwecke entfallen ersatzlos. Betroffen sind beispielsweise das „Listenprivileg“ und die Erlaubnis zum Adresshandel. Gleiches gilt auch für die Ausnahmeregelung von öffentlich zugänglichen Daten.

Werbemaßnahmen werden zukünftig noch mehr als bisher auf eine Einwilligung oder eine Interessensabwägung gestützt werden müssen. Das gilt nicht nur für B2C sondern auch für B2B. Bei der Interessensabwägung ist zu beachten, dass die berechtigten Interessen des Unternehmen im Rahmen der in Abschnitt 2 ausgeführten Informationspflichten gegenüber den betroffenen Personen offengelegt werden müssen.

Angesichts dieser grundlegenden Änderungen, empfiehlt es sich, sämtliche Aktivitäten auf ihre zukünftige Rechtmäßigkeit zu überprüfen. Fehlt eine legitimierende Rechtsgrundlage drohen Bußgelder bis zu 20 Mio. Euro und Schadensersatzansprüche der Betroffenen für materielle oder immaterielle Schäden etwa für den mit der Verarbeitung einhergehenden Grundrechtseingriff.

Die Wettbewerbsvorschriften im UWG sowie die Regelungen im Telekommunikationsrecht und für Telemediendienste (Webseiten, Webstatistiken) bleiben grundsätzlich bestehen.

Auch für die Prozesse und Abläufe im Unternehmen gibt es neue gesetzliche Vorgaben. Betroffen sind alle Prozesse, in denen personenbezogene Daten von Kunden, Mitarbeitern, Bewerbern, Interessenten, Geschäftspartner und allen anderen Personen verarbeitet werden. Tabelle 2 (siehe unten) fasst die wesentlichen Anforderungen zusammen.

Auf den ersten Blick kommen die Prinzipien vertraut oder auch selbstverständlich vor. Neu ist, dass ihre Umsetzung bußgeldbewehrt ist. Tabelle 3 (Seite 32) zeigt an Hand von Beispielen, wie kurz der Weg zu einem Verstoß sein kann.

5. Neue Anforderungen in der IT-Sicherheit

Die DS-GVO erhöht die Vorgaben zur IT-Sicherheit gegenüber dem BDSG deutlich. Beim Outsourcing ist im Unterschied zum BDSG der Auftragnehmer selber verantwortlich, die von der DS-GVO aufgestellt Vorgaben einzuhalten (siehe auch Abschnitt 3). Unternehmen, die konzeptlos technische und organisatorische Maßnahmen aneinanderreihen, werden sich zukünftig anstrengen müssen, die neuen Vorgaben einzuhalten. Die DS-GVO verlangt eine dokumentierte Abwägung und Begründung der Sicherheitsmaßnahmen (IT-Sicherheitskonzept).

Als Ausgangspunkt dient der „Stand der Technik“, das heißt technische und organisatorische Maßnahmen müssen sich beispielsweise. an der aktuellen Produktgeneration oder Programmversion sowie etablierten Standard und Normen (siehe Abschnitt 6) orientieren. Dabei darf nur in begründeten Fällen auf „veraltete“ Maßnahmen zurückgegriffen werden. Für die Entscheidung für und gegen Maßnahmen verlangt die DS-GVO von Unternehmen, abzuwägen zwischen

- den Implementierungskosten,
- der Verarbeitungsart,
- dem Verarbeitungsumfang,
- den Umständen und den Zwecken der Verarbeitung sowie
- der Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten der von der Verarbeitung betroffenen Personen (Mitarbeiter, Nutzer, Kunden, Lieferanten usw.).

Die Konzeption sowie deren Umsetzung wird regelmäßig anzupassen sein, da sich der Stand der Technik wie auch der Stand der „Angriffstechnik“ ändert, die zu neuen Risiken für die betroffenen Personen führen kann. Führ die Risikobetrachtung müssen auch Risiken durch ungewollte Ereignisse berücksichtigt werden:

- Datenvernichtung,
- Datenverlust,
- Datenveränderung,
- unbefugte Weitergabe und
- unbefugter Zugang.

Mit der Pflicht, die Wirksamkeit der Maßnahmen regelmäßig zu testen, greift die

TABELLE 2

Überblick über gesetzliche Vorgaben an Prozesse und Abläufe

Prinzip	Vorgabe
Daten Minimierung	• für den Zweck angemessen • sachlich relevant • auf notwendiges Maß beschränkt
Richtigkeit der Daten	• sachlich richtig • neuester Stand (falls für Zweck erforderlich) • Löschung oder Berichtigung unzutreffender Daten
Erforderlichkeit des Personenbezugs	• Speicherung des Personenbezug nur wenn für Zwecke erforderlich (z.B. nicht für statistische Zwecke)
Zweckbindung	• Sicherstellen, dass nur Daten nur für erlaubte Zwecke verarbeitet werden
Datengeheimnis	• Sicherstellen, dass mit der Verarbeitung betraute Personen ausschließlich gemäß Anweisungen handeln

TABELLE 3
Beispiele für Verstöße gegen die Prinzipien

Prinzip	Beispiel für Verstoß
Daten Minimierung	• Erhebung des Geburtsdatums bei Vertragsschluss
Richtigkeit	• Verwendung falscher oder veralteter Daten bei Bonitätsberechnung
Erforderlichkeit des Personenbezugs	• Einbeziehung des Namens bei der Berechnung der Anzahl an Kunden pro Monat
Zweckbindung	• Adhoc-Analyse durch Marketing ohne Genehmigung ohne Rechtsgrundlage
Datengeheimnis	• Verwendung von Kundendaten für private Versicherungsvermittlung durch Mitarbeiter

DS-GVO die Erkenntnis auf, dass nur wirksam ungesetzte Maßnahmen Schutz bieten.

Grundsätzlich muss jeder Sicherheitsvorfall dokumentiert werden. Ab einer definierten Schwere ist zusätzlich die Datenschutzaufsichtsbehörde spätestens nach 72 Stunden ab Kenntnisnahme zu unterrichten. Bei besonders schwerwiegenden Vorfällen müssen zusätzlich alle betroffenen Personen informiert werden. Die Aufsichtsbehörden können die im Rahmen der Meldung erlangten Informationen auch zu Einleitung eines Bußgeldverfahrens, zum Beispiel wegen unzureichender Sicherheitsmaßnahmen, verwenden. Es besteht kein Verwertungsverbot! Eine unterlassene Meldung ist ebenfalls bußgeldbewehrt. Wirksame und angemessene Sicherheitsmaßnahmen helfen dieses Dilemma zu vermeiden.

Ein Sicherheitsvorfall liegt vor, wenn personenbezogene Daten
- zufällig oder unrechtmäßig
  - zerstört werden,
  - verloren gehen,
  - verändert werden oder
- unbefugt
  - offenbart werden,
  - Zugang gewährt wird,
  - übermittelt werden,
  - gespeichert werden oder
  - anderweitig verarbeitet werden.

Erfasst sind damit grundsätzlich alle Spielarten der unbefugten Verarbeitung wie etwa Abfrage der Kundendatenbank für private Zwecke durch Mitarbeiter oder das unbefugte Vernichten von Backupmedien.

Eine zufällige Verletzung liegt unter anderem bei einem Festplattendefekt vor, in dessen Folge Kundendaten zerstört werden, die nicht anderweitig gespeichert sind. Beispielsweise ist der vorübergehende Ausfall eines Servers kein Sicherheitsvorfall.

6. Standards und Normen

Vereinigungen können Standards zum Datenschutz entwickeln und, soweit sich Unternehmen zu ihrer Einhaltung verpflichten, deren Einhaltung kontrollieren. solche Standard müssen von den Datenschutzaufsichtsbehörden anerkannt werden. Hierbei handelt es sich um Regelungen wie zum Beispiel den Code of Conduct der Versicherungswirtschaft. Zu einem solchen Standard im Bereich des Outsourcings/der Auftragsverarbeitung könnte zum Beispiel auch der von GDD und BvD vorgelegte Standard zur Auftragsdatenverarbeitung entwickelt werden.

Ausdrücklich geregelt ist auch die Zertifizierung. Zertifizierungsstellen bedürfen gesonderten einer Akkreditierung gemäß der DS-GVO, deren Modalitäten der deutsche Gesetzgeber noch festlegen muss. Gerade im Rahmen der Auftragsverarbeitung gewinnt sie in unterschiedlicher Hinsicht Bedeutung. Zum einen kann sie im Verhältnis zum Auftraggeber wie auch die Einhaltung von Standards als Nachweis für die Einhaltung datenschutzrechtlicher Vorgaben herangezogen werden. Zum anderen dienen beide Instrumente den eigenen Nachweispflichten eines Auftragsverarbeiters oder eines datenverarbeitenden Unternehmens zur Einhaltung der ihm obliegenden Datenschutzverpflichtungen. Und zum dritten kann eine bestehende Zertifizierung wie auch die Einhaltung von Standards im Bußgeldverfahren zugunsten eines datenverarbeitenden Unternehmens oder eines Auftragsverarbeiters wirken.

7. Erste Schritte zur erfolgreichen Umsetzung

Erste Schritte auf dem Weg zur Umstellung auf die DS-GVO sind
- Information der relevanten Akteure (Geschäftsführung, Fachabteilungen, IT, Betriebsrat)
- Aufbau oder Einkauf von Fachwissen über die Anwendung der DS-GVO
- Erhebung des Ist-Zustands unter anderem mit
  - Prozessen und ihrer Beschreibung (beispielsweise QM-Handbücher),
  - Zwecken für jedes Datenfeld,
  - Rechtsgrundlagen für jedes Datenfeld und
  - Einschlägigen Löschfristen,
- Aufbau eines Datenschutzmanagementsystems
- Aufbau oder Ausbau eines Dokumentationssystems
- Prüfung und Anpassung der Rechtsgrundlagen an DS-GVO
- Anpassung aller Verträge zur Auftragsdatenverarbeitung
- Prüfung und Anpassung der IT-Sicherheitsmaßnahmen.

Angesichts des hohen Anpassungsbedarfs erscheint die zweijährige Übergangszeit eher zu kurz als zu lang.

Dr. Niels Lepperhoff und Thomas Müthlein

Dr. Niels Lepperhoff (links) ist Geschäftsführer der Xamit Bewertungsgesellschaft, Thomas Müthlein ist Geschäftsführer der DMC Datenschutz.