STIFTUNG DATENSCHUTZ

AKTUALISIERTE FASSUNG ZUR EU-DATENSCHUTZ-GRUNDVERORDNUNG

KOMMUNIKATION VON DATENSCHUTZ – RECHT UND (GUTE) PRAXIS

Datenschutzkommunikation als Wettbewerbsvorteil und Verwaltungsservice

Gefördert durch

DATEV STIFTUNG Zukunft

Partner

UNIVERSITÄT PASSAU

STIFTUNG
DATENSCHUTZ

Stiftung Datenschutz
rechtsfähige Stiftung bürgerlichen Rechts
Karl-Rothe-Straße 10–14
04105 Leipzig
Deutschland

Telefon 0341 / 5861 555-0
mail@stiftungdatenschutz.org
www.stiftungdatenschutz.org

gestiftet von der Bundesrepublik Deutschland
vertreten durch den Vorstand Frederick Richter

Vorwort

Als Bundestiftung zur Förderung des Datenschutzes werden wir oft gefragt, wie wir konkret helfen können. Deshalb unterstützen wir gern die Publikation dieses Leitfadens für eine gute Datenschutzkommunikation. Denn aus unserer Praxis wissen wir, wie schwierig es gerade für kleinere Unternehmen, Vereine und Verbände häufig ist, Datenschutz als einen handfesten (Wettbewerbs-)Vorteil zu verstehen und nicht etwa – wie es leider oft geschieht – als Hindernis und lästige Pflicht. Eine klare Kommunikation kann hier Vertrauen schaffen und Kundenbeziehungen verbessern. Das erkennen immer mehr Unternehmen und Einrichtungen für sich. Für sie ist diese Handreichung bestimmt: Unser Material soll helfen, die Kommunikation zum Datenschutz transparent zu machen und juristische Fallstricke zu beseitigen.

Wir sind überzeugt, dass der Schutz der Privatsphäre weiter an Bedeutung gewinnen wird. Außerdem sehen wir den Datenschutz nicht – wie so viele – als lästige Bürokratie und Investitionshindernis, sondern als Voraussetzung für ein vertrauensvolles Miteinander und langfristig erfolgreiche Beziehungen in Wirtschaft und Gesellschaft. Dass wir mit dieser Auffassung nicht alleinstehen, erfahren wir immer öfter auf unseren Veranstaltungen, wenn Akteure aus Wirtschaft, Datenschutzaufsicht, Wissenschaft und Politik miteinander ins Gespräch kommen und ihre jeweiligen Ansichten und Interessen besser kennenlernen.

Ein Beispiel für einen solchen erfolgreichen Austausch ist diese Handreichung. Prof. Dr. Kai von Lewinski und Dirk Pohl, LL.B. (London) von der Forschungsstelle für Rechtsfragen der Digitalisierung (FREDI) an der Universität Passau haben die wichtigsten Aspekte der Datenschutzkommunikation juristisch und kommunikationswissenschaftlich fundiert und vor allem allgemein verständlich zusammengestellt, ermöglicht durch die Förderung der DATEV-Stiftung Zukunft. Mit der vorliegenden Fassung liegt bereits die zweite, auf die EU-Datenschutz-Grundverordnung angepasste Auflage vor. Deren Anliegen ist es ausdrücklich, den Text allen Interessierten zur freien Verwendung verfügbar zu machen, damit die Ergebnisse der Allgemeinheit zugutekommen. Wir freuen uns, dass wir dieses Anliegen unterstützen dürfen.

Naturgemäß unterliegen die Inhalte der Veränderung, und so haben wir uns dafür entschieden, auf eine gedruckte Publikation zu verzichten und die jeweils jüngste Version auf unserer Website zu veröffentlichen. Gern nehmen wir Ihre Anregungen und Verbesserungsvorschläge auf. Schreiben Sie uns, wir würden uns freuen: mail@stiftungdatenschutz.org.

Frederick Richter
Vorstand

Geleitwort

Das Datenschutzrecht ist geprägt von „rationaler Apathie“. Für die Betroffenen ist es oder scheint es nicht nur günstiger, Datenschutzverletzungen oder informationelle Zudringlichkeiten von Datenverarbeitern hinzunehmen, sondern auch, sich mit der Tatsache und den Rahmenbedingungen personenbezogener Datenverarbeitung überhaupt nicht zu befassen. Ursache hierfür ist zu einem großen Teil ein Informationsgefälle zwischen Verarbeiter und Betroffenem, zum Teil auch der Informationsfluss selbst.

Das Datenschutzrecht will dem durch gesetzliche Unterrichtungs-, Benachrichtigungs- und Auskunftspflichten begegnen. Doch sind diese Transparenzvorschriften selber länger als durchschnittliche Datenschutzerklärungen, konterkarieren also ihren Zweck der Transparenzermöglichung für Betroffene. Auch sonst werden Datenschutzinformationspflichten als für Verarbeiter und Betroffenen lästig verstanden, denen einerseits formal genügt und andererseits mechanisch durch Wegklicken ausgewichen wird.

Datenschutzkommunikation muss aber mehr sein und ist nicht nur die Erfüllung lästiger rechtlicher Pflichten. Datenschutz kann durch Privacy Policies und Codes of Conduct proaktiv Teil der Unternehmenskommunikation sein, Datenschutzerklärungen im Internet können interaktiv gestaltet werden, und Datenschutzsiegel und Zertifizierungen können Orientierung geben. Auch nach Ende des eigentlichen Verarbeitungszwecks ist Datenschutzkommunikation noch nicht zu Ende: Meldung von Datenpannen und Datenschutz-Mediation sind nicht nur rechtlich, sondern auch kommunikativ herausfordernd.

Diese aktualisierte Publikation enthält einen rechts- und kommunikationswissenschaftlich fundierten, mit den praktischen Bedürfnissen abgeglichenen und allgemeinverständlichen Erläuterungstext. Er steht unter einer freien Lizenz der Allgemeinheit zur Verfügung und kann in der Praxis, für Schulungen und Weiterbildung und von jedermann verwendet werden. Seine Entstehung verdankt er auch der Förderung durch die DATEV-Stiftung Zukunft.

Prof. Dr. Kai von Lewinski
Lehrstuhl für Öffentliches Recht, Medien- und Informationsrecht an der Universität Passau

Grußwort

Als die DATEV-Stiftung Zukunft durch die DATEV eG ins Leben gerufen wurde, war es bei der Festlegung des Stiftungszwecks ein besonderes Anliegen Datenschutz und IT-Sicherheit fest darin zu verankern. Denn als Genossenschaft der steuerberatenden, wirtschaftsprüfenden und rechtsberatenden Berufe sieht die Stifterin die Wissensvermittlung und Sensibilisierung zu diesen Themen in der breiten Öffentlichkeit als unerlässlich an.

Die digitale Transformation hat nahezu in allen wirtschaftlichen Bereichen Einzug gehalten und stellt nun Unternehmen und Kanzleien vor neue Herausforderungen. Bei der digitalen Verarbeitung von Daten ist es entscheidend für den Unternehmenserfolg, dass alle Mitarbeiter die Abläufe und Zusammenhänge verstehen und auch das Wissen haben, um die vertrauenswürdigen Daten zu schützen.

Aus diesen Gründen war die Initiative „Datenschutzkommunikation“ an der Universität Passau eines der ersten Projekte, die von der DATEV-Stiftung Zukunft gefördert wurden. Es zeigt sich in der Praxis in vielerlei Hinsicht, dass die Beachtung und Einhaltung gesetzlicher Pflichten ungeachtet ihrer Sinnhaftigkeit allzu häufig als lästiges Übel abgetan bzw. als nicht zu durchdringendes Dickicht von Vorschriften empfunden wird. Viele Menschen und Unternehmen vermissen einen fundierten und zugleich einfachen Zugang zu verständlichen Beispielen und Erläuterungen rund um dieses wichtige Rechtsgebiet. Deswegen freuen wir uns sehr, dass mit unserer Unterstützung nun diese Unterlage erstellt wurde, die dabei helfen soll die Sicherheit von den eigenen und auch fremden Daten in einer digitalen Zukunft zu bewahren. Wir wünschen der Initiative eine breite Beachtung in der Praxis!

Eckhardt Schwarzer
Vorstandsvorsitzender der
DATEV-Stiftung Zukunft

Julia Bangerth
Stv. Vorstandsvorsitzender der
DATEV-Stiftung Zukunft

Dr. Markus Algner
Vorstand der
DATEV-Stiftung Zukunft

Datenschutzkommunikation

Die Kommunikation im Bereich des Datenschutzes ist fordernd: Nicht nur die Datenverarbeiter (in der Gesetzessprache: „Verantwortlicher“, früher auch „Verantwortliche Stellen“) stöhnen unter den Informationspflichten und die Betroffenen dann unter den zur Verfügung gestellten Informationen. Auch der Gesetzgeber scheint konzeptionell noch keinen rechten Zugriff auf diesen Fragenkreis gefunden zu haben, was sich daran zeigt, dass die gesetzlichen Vorschriften, die die Kommunikation über Datenschutz anordnen, nahezu unlesbar und nur für Fachleute verständlich sind. In der Fachwelt werden zunehmend einzelne Vorschriften als fehlkonstruiert und kaum lesbar bezeichnet. Gerade die Informierungsvorschriften selber (z.B. Art. 13, 14 EU-Datenschutz-Grundverordnung [DSGVO]; §§ 32 ff. Bundesdatenschutzgesetz [BDSG]) sind häufig länger als durchschnittliche Datenschutzerklärungen und sind damit selbst kein rechtes Vorbild für Transparenz.

Im Folgenden soll gezeigt werden, wie man die rechtlichen Vorgaben im Bereich des Datenschutzes (I.) unter kommunikationspraktischen Erkenntnissen sinnvoll und insbesondere unter Berücksichtigung der praktischen Bedürfnisse umsetzen kann.

Die Darstellung vollzieht hierfür die unterschiedlichen Phasen der möglichen Kommunikation zwischen Verarbeiter und Betroffenen chronologisch nach. So beginnt die Auseinandersetzung mit den proaktiven Aspekten (II.), die der eigentlichen Kommunikation vorgelagert stattfinden müssen. Dieser folgen verschiedene, in der Regel rechtlich vorgegebene spezifische Kommunikationsanlässe (III.). Schlussendlich darf auch eine Auseinandersetzung mit dem „Worst Case“ eines Datenschutzverstoßes und der dann erforderlichen reaktiven Krisenkommunikation nicht fehlen (IV.).

In den einzelnen Abschnitten soll dabei jeweils zuerst auf die rechtlichen Form- und Verfahrenserfordernisse und die verlangten (Mindest-)Inhalte und dann auf mögliche Ansatzpunkte für eine für Verarbeiter und Betroffenen Vorteile bietende Kommunikationsstrategie eingegangen werden.

Inhaltsverzeichnis

I. Grundlagen

1. Rationale Apathie der Betroffenen

Ausgangspunkt für die Probleme der Kommunikation von Datenschutz ist die „rationale Apathie“ der Betroffenen. Für die Betroffenen scheint es oft günstiger, Datenschutzverletzungen oder informationelle Zudringlichkeiten von Datenverarbeitern hinzunehmen, ja sogar, sich mit der Tatsache und den Rahmenbedingungen personenbezogener Datenverarbeitung überhaupt nicht zu befassen. Ursache hierfür ist neben der schieren Informationsmenge das Informationsgefälle zwischen Verantwortlicher Stelle und Betroffenem, zum Teil auch der Informationsfluss selbst.

Eine ähnliche Apathie gegenüber dem Datenschutz scheint auch bei vielen Datenverarbeitern zu bestehen (s. bspw. ZEW Branchenreport Informationswirtschaft, http://t1p.de/yahx); sie kann jedoch aufgrund der gravierenden drohenden Konsequenzen bei diesen heute kaum mehr als rational begriffen werden.

a) „Information Overkill“

So hat die Menge der heutzutage verarbeiteten Informationen ein nur noch schwer in vorstellbaren Einheiten zu verbildlichendes Ausmaß erreicht. Auch haben Datenverarbeiter einen oft schwer kompensierbaren Kenntnis- und Informationsvorsprung. Der Gesetzgeber versucht dies in vielen Bereichen durch detaillierte Informationspflichten auszugleichen; am Beispiel von Beratungsprotokollen von Bankberatern etwa zeigt sich aber, dass umfangreiche Mitteilungs- und Dokumentationspflichten dem Verbraucher im Zweifel nicht helfen, wenn ihm eine Prüfung der mitgeteilten Informationen entweder aufgrund der Masse oder fehlender Fachkenntnisse ohnehin kaum möglich ist. – Man umschreibt dieses Phänomen häufig mit dem Begriff „information overkill“.

b) Fehlende Fühlbarkeit informationeller Eingriffe

Hinzu kommt, dass informationelle Eingriffe nicht unmittelbar fühlbar sind. Sie haben meist keine direkte Konsequenz. Der Mensch reagiert auf solchermaßen gemittelte Reize und Impulse weniger stark als etwa auf körperlichen Schmerz oder eine unmittelbare finanzielle Einbuße. Somit ist es schon aus psychologischer Perspektive verständlich, dass Gefährdungen und Verletzungen der informationellen Privatheit als weniger dringlich empfunden werden als Beeinträchtigungen durch die physische Umwelt. Zudem finden die häufigsten Verstöße auf einer sehr niederschwelligen Ebene statt (insb. im Werbebereich und im Internet), sodass von rechtlichen Schritten meist nicht nur abgesehen wird, sondern diese gar nicht erst als eine Option wahrgenommen werden. Ein weiterer Faktor ist die Gewöhnung an die Weitergabe von Daten im „Umsonst-Internet“, bei dem die Daten gewissermaßen im Tausch gegen Inhalte oder Dienste abgegeben werden.

c) Lästigkeit des Datenschutzes

Solange der Betroffene Datenschutzinformation und Datenschutz jedoch nicht für wichtig hält, befindet man sich schlussendlich in der Situation, dass der Datenschutz nicht nur für die Verantwortliche Stelle, sondern auch für den Betroffenen lästig ist. Der eine versucht daher, den Vorgaben formal zu genügen, während der andere den Informationen, soweit es geht, mechanisch durch Wegklicken und Wegwischen ausweicht.

d) Datenschutz als dysfunktionales Argument

Dem Ruf des Datenschutzes ist es wenig dienlich, dass er teilweise als dysfunktionales Argument missbraucht wird. Durch das Informationsfreiheitgesetz des Bundes (IFG) und weitere auf Landesebene ist mittlerweile im öffentlichen Bereich ein Wandel von grundsätzlichem Aktengeheimnis und Vertraulichkeit der Verwaltung hin zu einer Transparenz und einem grundsätzlich freien Zugang zu Informationen zu erkennen. Der Datenschutz wird hier aber – wie teils auch das Urheberrecht – berechtigten Informations- und Transparenzpflichten pau-

schal entgegengehalten. Freilich sind Fälle denkbar, in denen dies zum Schutze persönlicher Daten Dritter unumgänglich ist. Eine pauschale Ablehnung aufgrund datenschutzrechtlicher Bedenken verhindert aber die Befassung mit dem Einzelfall. Der Datenschutz soll gerade den Interessen des Individuums dienen und nicht zur Abwehr ebenfalls bestehender Informationsansprüche missbraucht werden. – Hier wird Datenschutz ein Argument des Verarbeiters und damit sinnverkehrt.

2. (Verfassungsrechts-)Gründe für den Datenschutz

Wenn man von etwas nichts weiß, dann macht es einen auch nicht heiß. – Notwendige Voraussetzung für aufgeklärtes Handeln im Bereich moderner Datenverarbeitung ist, dass die Betroffenen die informationellen Zugriffe oder die entsprechende Verarbeitung erkennen können.

Das Betroffenenleitbild des Datenschutzrechts weist viele Parallelen zum Verbraucherschutz auf. Ausgangspunkt ist ein strukturelles Informationsungleichgewicht sowie der potentielle „information overload". Der Betroffene wird als grundsätzlich schutzbedürftig angesehen, da er der oben (1.) beschriebenen rationalen Apathie unterliegt. Dabei beschränkt sich der Schutz des Datenschutzrechtes nicht nur auf das Verhältnis zwischen Individuum und Staat, sondern soll dem Betroffenen insbesondere – wie auch der Verbraucherschutz – Rechte gegenüber Privatunternehmen einräumen.

a) „Informationelle Selbstbestimmung" als Grundrecht

***Franzius**, Das Recht auf informationelle Selbstbestimmung, ZJS [Zeitschrift für das juristische Studium] 2015, S. 259 ff. abrufbar unter: http://t1p.de/6bx7 [ZJS, kostenfrei].*

Das Datenschutzrecht will den Betroffenen zunächst einmal überhaupt in den Stand versetzen, seine informationellen Interessen und Belange wahrzunehmen. Da informationelle Eingriffe nicht fühlbar sind und sich – wenn überhaupt – erst mit Zeitversatz bemerkbar machen, ist es eine Notwendigkeit, dass der Betroffene über die Verarbeitung seiner Daten informiert und orientiert ist.

Zwar wird als Leitbild des Datenschutzes häufig die Selbstbestimmung des Individuums angeführt, was bezüglich der Einwilligungsmöglichkeiten des Betroffenen auch nicht von der Hand zu weisen ist. Andererseits zeichnet sich die gewählte Regelungsmethode eines Verbots der Verarbeitung personenbezogener Daten mit Erlaubnisvorbehalt aber stark dadurch aus, dass hier vor allem Dritten Grenzen für die Verarbeitung gesetzt werden. Freiheit und Freiraum zur informationellen Selbstbestimmung soll zunächst einmal durch diese „Fremdbeschränkung" geschaffen werden (zu diesem Konzept v. Lewinski, „Die Matrix des Datenschutzes", Mohr Siebeck 2014, S. 46).

Ausgangspunkt war für den Datenschutz in Deutschland aus rechtlicher Sicht die Idee der „Informationellen Selbstbestimmung" über die personenbezogenen Daten aus dem Volkszählungsurteil des Bundesverfassungsgerichts (Amtliche Sammlung [BVerfGE], Bd. 65, S. 1 ff.). Dieses leitete aus dem allgemeinen Persönlichkeitsrecht ein „Recht auf informationelle Selbstbestimmung" her. Der Einzelne solle selber darüber bestimmen können, wer seine Daten erhält und verarbeitet und gegen die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten geschützt werden. In den Schutzbereich der informationellen Selbstbestimmung fallen dabei alle Formen der Verarbeitung personenbezogener Daten.

Die Europäisierung des Datenschutzrechts hat zur Folge, dass das Recht auf informationelle Selbstbestimmung nun durch das Datenschutzgrundrecht aus Art. 8 Abs. 1 der Charta der Europäischen Grundrechte (EU-GRCh) teilweise verdrängt wird. Ob sich hieraus wesentliche Änderungen ergeben, wird unterschiedlich

gesehen. Jedenfalls ist nunmehr auch der freie Verkehr personenbezogener Daten als Schutzziel ausdrücklich anerkannt (Art. 1 Abs. 1 a.E. DSGVO), womit der unternehmerischen Freiheit der Verarbeiter aus Art. 15 EU-GRCh Rechnung getragen wird.

b) Einwilligung

Die Einwilligung in die Verarbeitung von Daten gibt dem Einzelnen die Möglichkeit, eine Verarbeitung seiner Daten zu gestatten. Hier geht es vorrangig um die eigentliche Ausübung informationeller Freiheit und nicht primär um die Kontrolle der Datenverarbeitung durch andere. Damit hier auch nur bewusste Entscheidungen berücksichtigt werden, werden an die Freiwilligkeit und die Eindeutigkeit der Einwilligung hohe Anforderungen gestellt. Gleichzeitig stellt die Einwilligung aus Verarbeitersicht in der Praxis aber das flexibelste Werkzeug für die rechtmäßige Verarbeitung von Daten außerhalb der (beschränkten) gesetzlichen Erlaubnisnormen dar. Zwar ist eine Rechtfertigung einer Verwendung zu Werbezwecken über ein berechtigtes Interesse des Verarbeiters möglich, aber auch dieser Erlaubnistatbestand hat bei der Verarbeitung von besonderen personenbezogenen Daten eine Grenze, weil die Einwilligung in diesem Fall zwingend einzuholen ist.

c) Gesetzliche Erlaubnistatbestände

Im Interesse der Allgemeinheit und Dritter hat das Bundesverfassungsgericht schon zum Zeitpunkt der Volkszählungs-Entscheidung im Jahre 1983 Ausnahmen vom generellen Verbot der Datenverarbeitung zugelassen und festgestellt, dass dieses Recht des Einzelnen nicht absolut gelten kann. In Anbetracht der technischen und gesellschaftlichen Realität einer allgegenwärtigen Datenverarbeitung scheint dies auch kaum anders denkbar. So ist es alternativ zur Einwilligung erlaubt, dass derjenige, der personenbezogene Daten verarbeitet, sich hierfür auch auf eine gesetzliche Grundlage stützen kann. Diesem Konzept des „Verbots mit Erlaubnisvorbehalt“ folgt auch die DSGVO (vgl. Art. 6 DSGVO).

d) Flankierende Informationspflichten

Unabhängig von dem Rechtsgrund für eine personenbezogene Datenverarbeitung – Einwilligung oder gesetzliche Gestattung – setzt das Datenschutzrecht zum Schutz personenbezogener Daten des Einzelnen insbesondere bei den Informierungen an und will bestehende Wissensdefizite der Betroffenen verringern. Ohne Kenntnis davon, wer was über ihn weiß, können Betroffene ihre Rechte nicht wirksam geltend machen.

Herkömmliche Mittel hierzu sind die Unterrichtung bei der Datenerhebung, die nachträgliche Benachrichtigung oder die Auskunft auf Verlangen des Betroffenen. Letztere setzt natürlich schon eine gewisse Kenntnis oder zumindest Vermutung über eine mögliche Datenverarbeitung voraus. Hinzu kommen vereinzelt Kennzeichnungspflichten und öffentliche Bekanntmachungen von Datenpannen.

Eine funktionierende Datenschutzstrategie ist unter der neuen DSGVO nun zur echten Rechtspflicht geworden (vgl. Art. 24 DSGVO). Verantwortliche Stellen müssen nunmehr vor Beginn der Datenverarbeitung ein Verzeichnis mit Verarbeitungstätigkeiten anlegen (Art. 30 DSGVO). Darunter fallen auch Maßnahmen zur Datensicherheit. Zudem illustriert die Pflicht vor risikoreichen Verarbeitungstätigkeiten eine Datenschutzfolgenabschätzung durchzuführen, dass sich Verarbeiter ein konkretes Vorstellungsbild über den Datenschutz machen müssen. Letztlich bauen hierauf auch die Kommunikationspflichten der DSGVO auf. Diese erklären die Transparenz der Verarbeitung (Art. 5 Abs. 1 lit. a DSGVO; ErwGr. 39, 58 u. 78) und insbesondere die Transparenz gegenüber den Betroffenen (Art. 12 DSGVO) – auch bei Ausübung seiner Betroffenenrechte gem. Art. 15 ff. DSGVO – zu Grundpflichten für jede datenverarbeitende Stelle. Auch werden der Verantwortlichen Stelle in Art. 5 Abs. 2 DSGVO umfangreiche Rechenschaftspflichten (engl.: „accountability“) über die Einhaltung der Verarbeitungs- und Transparenzpflichten auferlegt.

3. Datenschutzgesetze

a) Die EU-Datenschutz-Grundverordnung

Wybitul, Die DS-GVO veröffentlicht – Was sind die neuen Anforderungen an die Unternehmen? ZD [Zeitschrift für Datenschutz] 2016, S. 253 ff. abrufbar unter: http://t1p.de/sluh [Beck-online, kostenpflichtig]

Die neue DSGVO entfaltet ihre rechtlichen Wirkungen ab dem 25. Mai 2018. Die Grundvorstellung des bisherigen deutschen Datenschutzrechtes bleibt unter der DSGVO erhalten: Die Verarbeitung von personenbezogenen Daten wird weiterhin im Grundsatz für schädlich gehalten. Es besteht deshalb regelungstechnisch ein Verbot mit Erlaubnisvorbehalt. Die Verarbeitung von personenbezogenen Daten ist verboten, solange sich die Verantwortliche Stelle nicht auf eine gesetzliche Erlaubnisnorm oder auf eine wirksame Einwilligung des Betroffenen berufen kann. Daneben gibt es umfangreiche Informationspflichten (Art. 13, 14 DSGVO). Tendenziell werden die Anforderungen an Verständlichkeit und Transparenz gegenüber dem bisherigen Datenschutzrecht erhöht. Insbesondere die Transparenz wird durch den Art. 5 Abs. 1 lit. a DSGVO zu einem zentralen Prinzip der Datenverarbeitung erklärt. Art. 12 DSGVO legt genauere Voraussetzungen für die Kommunikation bei der Erhebung von Daten und insbesondere für die Information über die Ausübung der Betroffenenrechte fest. Auch für die Wirksamkeit einer beim Betroffenen eingeholten Einwilligung scheint die DSGVO ein erhöhtes Maß an Transparenz und Verständlichkeit zu verlangen.

Daneben gilt inhaltlich ein strenger Maßstab. So muss die Einwilligung informiert erfolgen, und sie muss unmissverständlich sein. Die Formulierungen deuten darauf hin, dass Mängel in der Kommunikation im Zweifel zulasten der Verantwortlichen Stelle gehen, denn der Nachweis der nach obigen Bedingungen erfolgten Einwilligung obliegt ihr (Art. 7 Abs. 1 DSGVO).

b) Das Ziel der Vollharmonisierung und seine Ausnahmen

Auch in Zukunft trägt die Strukturierung der Datenschutzgesetze in Deutschland wenig zur Übersichtlichkeit des Datenschutzrechtes bei. So verteilten sich die anwendbaren Normen je nach Einzelfall über diverse europarechtliche Regelungen sowie Bundes-, Landes- und bereichsspezifische Spezialgesetze. Insbesondere die Abgrenzungen zwischen einzelnen Spezialgesetzen erweisen sich im Detail als schwierig.

Die bisher zentrale Unterscheidung für die Anwendbarkeit nach öffentlichen und nicht-öffentlichen Stellen sowie Spezialregelungen für bestimmte Datenkategorien werden durch die DSGVO größtenteils beseitigt. Für nicht-öffentliche Stellen – also die Wirtschaft – gilt im Grundsatz die DSGVO; man spricht hier von einer Vollharmonisierung. Die Verarbeitung durch öffentliche Stellen – also die Verwaltung – richtet sich grundsätzlich genauso nach Art. 6 DSGVO.

Aus zwei Gründen kann eine Unterscheidung aber nach Wirksamwerden der DSGVO noch nötig sein, soweit für den öffentlichen Bereich Öffnungsklauseln bestehen. In Art. 23 DSGVO findet sich eine Auflistung von diversen Bereichen des öffentlichen Sektors, in denen die Mitgliedsstaaten abweichende Regelungen erlassen könnten. Für den öffentlichen Bereich hat die Grundverordnung dadurch eher Richtliniencharakter. Art. 23 Abs. 2 DSGVO legt aber für diesen Bereich grundsätzliche datenschutzrechtliche Anforderungen fest, die im Geltungsbereich des Grundgesetzes auch unabhängig von der DSGVO zu beachten sind.

Eine weitere spezielle Ausnahme stellen die öffentlichen Stellen dar, die generell nicht der Anwendung des Unionsrechts unterfallen. Zu nennen sind hier das Bundesamt für Verfassungsschutz, der Bundesnachrichtendienst, der Militärische Abschirmdienst und der Bereich des Sicherheitsüberprüfungsgesetzes. Nicht unerwähnt bleiben sollte hier die Richtlinie (EU) 2016/680 „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufde-

ckung oder Verfolgung von Straftaten oder der Strafvollstreckung“. Für diesen Bereich wird es nach Umsetzung durch die Mitgliedsstaaten separate Regelungen geben. In Deutschland sind diese nunmehr ebenfalls im BDSG enthalten (§§ 45 ff. BDSG).

4. Datenschutz als Wettbewerbsvorteil und bessere Verwaltungsleistung

***Hoeren**, Datenschutz als Wettbewerbsvorteil, in: Bäumler (Hrsg.), E-Privacy, Vieweg und Teubner Verlag 2000, S. 263 ff.*

Gefällige Datenschutzkommunikation kann mehr sein als nur die Erfüllung lästiger rechtlicher Pflichten. Da den entsprechenden Pflichten nicht ausgewichen werden kann, mag eine Verantwortliche Stelle die Perspektive wechseln und überlegen, wie die Kommunikation wirtschaftlich und administrativ sinnvoll, d.h. als Vorteil im Wettbewerb oder zur Verbesserung der Verwaltungsleistung, genutzt werden kann. Die Vorteile einer gelungenen Kommunikationsstrategie liegen dabei nicht nur in der Abwehr von schlechter Presse und gesetzlicher Sanktionen, sondern es besteht auch ein Eigeninteresse des Verarbeiters.

a) Betroffenenvertrauen als Gut

***Mantelero**, Competitive value of data protection, IDPL [International Data Privacy Law] 2013, S. 229 ff. abrufbar unter http://idpl.oxfordjournals.org/content/3/4/229.full.pdf+html [Oxford Academic, kostenpflichtig]*

Neben den Kosten für die Umsetzung datenschutzrechtlicher Anforderungen darf die Steigerung des Vertrauens der Betroffenen auch bei einer betriebswirtschaftlichen und verwaltungspraktischen Betrachtung der Kommunikationsstrategie nicht außer Acht bleiben. Bei Missachtung der gesetzlichen Mindestanforderungen setzt man sich außerdem Haftungs- und Prozessrisiken aus.

Zwar wird der EU-Datenschutz-Grundverordnung und dem diese dann interpretierenden Europäischen Gerichtshof (EuGH) nicht ganz zu Unrecht unterstellt, dass die Interessen und Rechte des Einzelnen häufig höher bewertet werden als die Interessen der Unternehmen. Über die notwendige und transparente Kommunikation aus rechtlich zwingendem Anlass hinaus kann die Kommunikation im Datenschutz jedoch als Teil der Öffentlichkeitsarbeit ein handfester Marketingvorteil werden, indem man sich durch Fairness und Transparenz von anderen Verarbeitern abgrenzt. Das Datenschutzrecht macht nämlich nur – freilich auf hohem Niveau – Mindestvorgaben und belässt den Verantwortlichen Stellen Möglichkeiten für höhere Datenschutzstandards.

In einer Zeit, in der Daten immer mehr zu einem wirtschaftlichen Gut werden, ist der Zugriff auf diese von großer wirtschaftlicher und administrativer Bedeutung. Betroffene wird man langfristig nur durch Transparenz und Vertrauen dazu bringen können, Daten offenzulegen. Es kann dabei sinnvoll sein, ausdrücklich und in einer klaren Sprache den Vorgang der Datenverarbeitung transparent zu machen. Insbesondere bei datengetriebenen Anwendungen sind die Vorteile hervorzuheben, die ggf. dadurch entstehen, dass der Verarbeiter mehr Informationen über den Betroffenen hat. Das Vertrauen in die Verantwortliche Stelle ist insbesondere von elementarer Bedeutung, da deren Kommunikation letztendlich den einzigen nachprüfbaren Ansatzpunkt für den Betroffenen darstellt: Die Überprüfung, ob die gemachten Angaben zum Umgang mit den Daten tatsächlich der Realität entsprechen, ist diesem kaum möglich, sondern allein den Datenschutzbehörden.

b) Datenschutzkommunikation als Instrument im Wettbewerb

Es gibt durchaus Konzepte, Informationen über Datenschutz verständlich und gefällig zu kommunizieren. Diese Anforderungen lassen sich aber nur schwer in „harte“ gesetzliche Regelungen gießen. Allerdings gibt es Wege, die unhandlichen „harten“ rechtlichen Verpflichtungen in eine eingängigere Form zu gießen. Wenn die Kommunikation von Datenschutz dann nicht mehr als Last empfunden wird, kann sie zu einem positiven Fak-

tor werden. Bei Betroffenen ist durch Datenskandale in der Vergangenheit zumindest in einigen Bereichen eine Sensibilisierung für das Thema zu erkennen. Dies gilt insbesondere für die Möglichkeiten eines späteren Zugriffs von Sicherheitsbehörden auf ursprünglich von Privaten oder der sonstigen Verwaltung zusammengestellte Datensammlungen.

Die Verantwortliche Stelle kann den Datenschutz dann als Wettbewerbsvorteil oder als Bürgerservice nutzen, wenn sie diesen statt als reine Erfüllung von gesetzlichen Pflichten und der Vermeidung von schlechter Presse als Teil der Öffentlichkeitsarbeit und als Qualitätsmerkmal für das Endprodukt ansieht. Die Einhaltung der Vorgaben des Datenschutzrechts an sich schafft dabei nur wettbewerbliche Gleichheit bzw. Compliance. Erst ein darüber hinausgehendes (zumindest kommunikatives) Engagement der Verantwortlichen lässt sich vorteilhaft nutzen.

Die Möglichkeiten, Datenschutzkommunikation flankierend als Instrument des Marketings zu verwenden, werden heute schon genutzt. Häufig endet dies aber in der Praxis darin, dass letztlich leere Floskeln, Wiederholungen der gesetzlichen Regelungen und bloße Selbstverständlichkeiten folgen, die durch weitgehende Ermächtigungen zur Verwendung der Daten die Datenschutzkommunikation in ihr Gegenteil verkehren.

Die Erstellung auch kommunikationspraktisch sinnvoller Texte stellt aufgrund der umfangreichen rechtlichen Vorgaben und der nötigen Ausführungen zu technischen Vorgängen keine einfache, aber eine lösbare Aufgabe dar. Ziel sollte die Verwendung von rechtswissenschaftlich und kommunikationstheoretisch fundierten, mit verarbeitungspraktischen Bedürfnissen abgeglichenen und allgemeinverständlichen Texten sein.

c) Datenschutzkommunikation zur Verbesserung der Verwaltungsleistung

***Wirtz/Göttel/Thomas/Langner**, Bürgerorientierte Web 2.0-Services, Deutsches Forschungsinstitut für die öffentliche Verwaltung, 2016*

Auch für öffentliche Stellen kann sich eine sinnvolle Kommunikation im Bereich des Datenschutzes als Vorteil erweisen. Freilich steht bei Stichwort „e-Government“ meist zuerst die Vereinfachung für die Verwaltung und die Steigerung von Effizienz und auch Effektivität im Vordergrund. Auch muss Verwaltung im Gegensatz zu im wirtschaftlichen Wettbewerb angebotenen Dienstleitungen in erster Linie nicht zielgruppenorientiert, sondern rechtmäßig ausgestaltet werden. Daneben kann die Digitalisierung jedoch dazu genutzt werden, den Kontakt mit der Verwaltung bürger- und unternehmensfreundlich zu gestalten. Über die ohnehin rechtlich verpflichtende transparente Datenschutzkommunikation hinaus, lassen sich viele der hier präsentierten Ansätze auch auf weiteres transparentes und bedarfsgerechtes Verwaltungshandeln übertragen. Verwaltung kann zum echten Bürgerservice werden, über Ansprüche, Rechte und Pflichten aufklären und die Rechtsstaatlichkeit stärken.

d) „Nudging“: Ein Konzept zur Verhaltenssteuerung

Nicht ganz neu, aber vieldiskutiert ist das Konzept des sog. „Nudging“. Eine gelungene deutsche Übersetzung hat sich noch nicht etabliert. Im wörtlichen Sinne könnte man hilfsweise die Bezeichnungen „Stupser“ oder „Anstoß“ verwenden.

Grundlage des Konzeptes ist die sanfte Beeinflussung von Verhalten. Dabei wird davon ausgegangen, dass wie oben bereits für den Datenschutz beschrieben (I.1.) der Mensch in der Regel keine streng rationalen ökonomischen Entscheidungen trifft, sondern für subjektive Anreize empfänglich ist und insofern häufig irrational handelt. Dieses Konzept kann im Marketing allgemein, aber auch insbesondere in der Datenschutzkommunikation zur Generierung von Wettbewerbsvorteilen und für eine bessere, bürgerorientierte Verwaltungsleistung von Nutzen sein.

Die Einsatzgebiete von „Nudges“ sind dabei vielfältig. So sollte bereits weithin bekannt sein, dass der Betroffene in der Regel dazu neigt, ihm vorgegebene Standardeinstellungen wie angekreuzte Kästchen beizubehalten und sich damit im Ergebnis der Vorgabe zu beugen, statt sich ausdrücklich dagegen zu entscheiden. Im Bereich der Einholung der Einwilligung sind dem freilich Grenzen gesetzt (I.2.b)), aber darüber hinaus sind derartige Gestaltungsmöglichkeiten nicht absolut ausgeschlossen. Je nach Einsatzzweck kann aber auch eine stärkere Individualisierung der Auswahlmöglichkeiten zu einer höheren Bindung führen. Dies beginnt schon bei einer persönlichen Ansprache in einem Text oder Video.

Gerade die Art der Informationsdarstellung kann schon im Vorfeld auf die eigentliche Entscheidung des Betroffenen Einfluss nehmen. Insbesondere neue und von anderen Arten der Darstellung abweichende Konzepte können Neugier wecken, solange sie trotz Neuheit intuitiv und übersichtlich sind.

Vor allem im Bereich öffentlicher Stellen sollte man jedoch aufgrund der intendierten Lenkungswirkung grundrechtliche Fragen nicht außer Acht lassen. Im privatwirtschaftlichen Bereich ergeben sich im Einzelfall werberechtliche Grenzen.

II. Proaktive Kommunikation

Auch wenn sich das Gesetz auf die individuelle Informierung des jeweiligen Betroffenen konzentriert, gibt es doch eine Reihe von Verpflichtungen, nach denen das Datenschutzniveau oder jedenfalls hierfür relevante Parameter an die Öffentlichkeit kommuniziert werden müssen. Der Fokus der gesetzlichen Regelungen der DSGVO liegt hier klar auf rein internen Prozessen, an welche jedoch im Rahmen der eigenen Kommunikationsstrategie angeknüpft werden kann. Zusätzlich sind innerhalb des Verfahrens bereits kommunikative Elemente mit dem Datenschutzbeauftragten, der Aufsichtsbehörde und den Betroffenen vorgesehen und teils sogar verpflichtend.

1. Interne Vorarbeiten

Durch die in den meisten Fällen vorzunehmende Compliance-Prüfung (Verzeichnis mit Verarbeitungstätigkeiten, Datenschutz-Folgenabschätzung) sind alle wesentlichen Informationen zur personenbezogenen Datenverarbeitung in Unternehmen bzw. Behörde aufbereitet. Es liegt nahe, sie für die Information von Markt und Öffentlichkeit zu nutzen. Soweit es von der Allgemeinheit positiv beleumundete Normwerke von Dritten (Verhaltensregeln, Zertifizierungsvorgaben, Siegel) gibt, können diese ebenfalls in die datenschutzkommunikative Öffentlichkeitsarbeit eingebaut werden.

Datenerfassung beim Aufruf von Webseiten

***Stiemerling/Lachenmann**, Erhebung personenbezogener Daten beim Aufruf von Webseiten, ZD [Zeitschrift für Datenschutz] 2014, S. 133ff. abrufbar unter: http://t1p.de/hc64 [beck-online, kostenpflichtig]*

Schon der Betrieb einer Webseite führt zu teils ungeahnten Verarbeitungsprozessen. Die folgende Liste soll einen Überblick über zu bedenkende Faktoren bieten:

- technisch notwendige Daten zum Aufruf der Website (insb. IP-Adresse)
- serverseitig erstellte Logfiles
- Temporäre und permanente Browser-Cookies
- Flash-Cookies
- Datenübertragungen an Dritte durch Plug-Ins (insb. sog. Analytics-Anbieter)
- Drittanbieter-Cookies (insb. Werbung, Like- oder Teilen-Buttons)
- Darüber hinaus angeforderte Daten (insb. Anmelde- und Kontaktformulare, Newsletter-Bestellung)

Gerade die Zahl von Drittanbieter-Inhalten ist selbst bei als seriös empfunden Websites häufig nicht niedrig. Browser-Erweiterungen wie „u block origin", „privacy badger" oder „CLIQZ" können hier einen ersten Anhaltspunkt für die Übermittlungen im Rahmen der eigenen Webpräsenz liefern. Notwendig ist im Anschluss eine Rücksprache mit dem für die technische Umsetzung Betrauten.

a) Verzeichnis der Verarbeitungstätigkeiten (DSGVO), vorm. Verfahrensverzeichnis (BDSG)

Im ganz ursprünglichen deutschen Datenschutzrecht wie im bisherigen europäischen Datenschutzrecht spielten Meldepflichten (gegenüber den Aufsichtsbehörden) eine wichtige Rolle. Im heutigen und noch geltenden deutschen Datenschutzrecht sind diese Meldepflichten als unnötige Bürokratie weitgehend abgeschafft. Sie bestehen nur noch hinsichtlich besonders risikoreicher Verarbeitungsverfahren (z.B. auch § 73 Abs. 1 S. 3 Messstellenbetriebsgesetz [MsbG]).

aa) Pflicht zum Verzeichnis von Verarbeitungstätigkeiten

Durch die DSGVO ist das bisher öffentlich zugängliche Verfahrensverzeichnis entfallen. In Art. 30 DSGVO ist nur noch ein sog. Verzeichnis von Verarbeitungstätigkeiten vorgesehen. Es ist als Ausgestaltung der oben bereits erwähnten Rechenschaftspflicht des Verarbeiters aus Art. 5 Abs. 2 DSGVO zu verstehen. Die Anforderungen an das Verfahrensverzeichnis unterscheiden sich dabei kaum von der Regelung des früheren BDSG. Weniger streng ist die Regelung durch eine teilweise Befreiung für Unternehmen mit weniger als 250 Mitarbeitern. Hier muss ein Verzeichnis nur für besonders risikoreiche, regelmäßig angewandte oder sensitive Daten betreffende Prozesse geführt werden. Soweit im Rahmen des Angebots einer App automatisiert Daten erhoben werden, dürfte eine regelmäßige und nicht nur gelegentliche Datenverarbeitung vorliegen, sodass ein Verfahrensverzeichnis zu führen ist.

Neu ist auch die Regelung der Verantwortlichkeit für die Führung des Verzeichnisses. Fiel diese Aufgabe bisher noch dem betrieblichen bzw. behördlichen Datenschutzbeauftragten zu, so wird sie durch Art. 30 Abs. 1 DSGVO der Unternehmensleitung zugewiesen. Eine Pflicht zur Führung eines solchen Verzeichnisses legt Art. 30 Abs. 2 DSGVO auch dem Auftragsverarbeiter auf.

bb) Inhaltliche Anforderungen

Die genauen Inhalte des Verzeichnisses werden in Art. 30 Abs. 1 lit. a–g DSGVO für den Verantwortlichen und in Art. 30 Abs. 2 lit. a–d DSGVO für den Auftragsverarbeiter detailliert aufgeführt. Hervorzuheben ist im Besonderen, dass die Verarbeitungszwecke in dem Verfahrensverzeichnis festgelegt werden müssen. Das heißt, der Verarbeiter muss sich über das „Ob" und „Warum" der Erhebung persönlicher Informationen Gedanken machen.

Durch die rein interne Verwendung erlischt die rechtliche Pflicht zur Kommunikation gegenüber Betroffenen und der Öffentlichkeit. Der Akzent liegt hier nunmehr wie auch schon bei der Folgenabschätzung primär auf einer rechtssicheren Kommunikation im Hinblick auf mögliche Prüfungen der Aufsichtsbehörden. Ein fehlendes notwendiges Verfahrensverzeichnis kann von der Aufsichtsbehörde sanktioniert werden (Art. 83 Abs. 4 DSGVO).

cc) Verwendung in der Datenschutzkommunikation

Es besteht aber freilich weiterhin die Möglichkeit, die ohnehin zu führenden und zu pflegenden Verarbeitungsverzeichnisse als Grundlage zur Erstellung umfassender und kommunikationswissenschaftlich fundierter Privacy Policies mit Werbewirkung zu nutzen. Im Rahmen der unten dargestellten Informierungspflichten (III.) sind teilweise auch Angaben über Art und Umfang der Verarbeitung rechtlich vorgeschrieben, die auf der Grundlage des Verarbeitungsverzeichnisses aufgearbeitet werden können.

b) Datenschutz-Folgenabschätzung (Art. 35 DSGVO)

***Wright/Finn/Rodrigues**, A Comparative Analysis of Privacy Impact Assessment in Six Countries, in: Journal of Contemporary European Research 9/1 (2013), S. 160 ff. abrufbar unter http://t1p.de/dico [JCER, kostenfrei]*

Durch die Datenschutz-Folgenabschätzung (engl.: „privacy impact assessment") in Art. 35 DSGVO wird den Verantwortlichen aufgetragen, bei Verarbeitungen mit einem hohen Risiko die Folgen für personenbezogene Daten im Voraus einzuschätzen. Art, Umfang, Umstände und Zweck der Verarbeitung sind hier Parameter, nach denen sich ein Risiko bemisst. Explizit nennt die DSGVO auch noch die Verwendung neuer Technologien. Risiken sollen erkannt und dann schon im Vorfeld der Verarbeitung durch geeignete Maßnahmen möglichst reduziert werden. Gefordert wird eine vertretbare Risikobewertung auf Basis der zum Zeitpunkt der Vornahme vorhandenen Informationen.

aa) Verfahren

Die ordnungsgemäße Durchführung einer Datenschutz-Folgenabschätzung wird vom betrieblichen bzw. behördlichen Datenschutzbeauftragten überwacht. Eine spätere Prüfung durch die Aufsichtsbehörden ist möglich.

Das vorgeschriebene Verfahren sieht dabei schon kommunikative Elemente vor: Einmal ist nach Art. 35 Abs. 2 DSGVO in jedem Fall auf Anfrage eine Beratung durch den betrieblichen bzw. behördlichen Datenschutzbeauftragen möglich. Hier lassen sich schon im Vorfeld geeignete Maßnahmen besprechen.

In bestimmten Fällen ist die Konsultation der Aufsichtsbehörden bei Erstellung der Datenschutz-Folgenabschätzung verpflichtend. Dies ist nach Art. 36 Abs. 1 DSGVO der Fall, wenn am Ende der Abschätzung ein hohes Risiko angenommen wird und die Verantwortliche Stelle nicht selber schon geeignete Maßnahmen zur Eindämmung trifft. Eine frühzeitige Abklärung möglicher Probleme als Grundgedanke der Folgenabschätzung kann gerade auch durch die Konsultation der Aufsichtsbehörden langfristig Verstöße vermeiden.

In Einzelfällen kann nach Art. 35 Abs. 9 DSGVO die Konsultation der Betroffenen notwendig werden. Dem Wortlaut der Norm nach scheint aber wohl ein Einholen der Standpunkte und eine Auseinandersetzung mit diesen zu genügen. Zwingend scheint die Konsultation jedoch nicht immer zu sein („gegebenenfalls"). Gerade bei größeren Gruppen von Betroffenen kann die Regelung kaum als Erfordernis eines direkten Kontakts mit den Personen, sondern nur als Möglichkeit der Einbeziehung von Interessenverbänden sinnvoll angewendet werden.

bb) Inhaltliche Anforderungen

Polnische Datenschutzaufsichtsbehörde, Liste der Verarbeitungen, für die eine Datenschutzfolge-Abschätzung notwendig ist, abrufbar unter http://t1p.de/v47m [in englischer Sprache]

Belgische Datenschutzaufsichtsbehörde, Liste der Verarbeitungen, für die eine Datenschutzfolge-Abschätzung notwendig ist, abrufbar unter http://t1p.de/1uk4 [in französischer Sprache]

Die Vorgaben der DSGVO für die Datenschutz-Folgenabschätzung sind dabei zu weiten Teilen organisatorischer Natur. Die inhaltlichen und damit für das Thema der Kommunikation entscheidenden Voraussetzungen finden sich vor allem in Art. 35 Abs. 7 DSGVO. So sollen die geplanten Verarbeitungsvorgänge, die Zwecke der Verarbeitung und ggf. die berechtigten Interessen des Verarbeiters „systematisch" beschrieben werden. Hier ist rechtlich vor allem auf die Abarbeitung der Mindestinhalte in Art. 35 Abs. 7 lit. b–d DSGVO zu achten und technisch auf genaue Beschreibungen der Vorgänge. Da es sich bei der Folgenabschätzung nicht um ein öffentlich zugängliches Dokument handelt, muss die Transparenz und Verständlichkeit aus rechtlicher Sicht nicht auf den Durchschnittsleser abstellen. Zielgruppe der Kommunikation sind hier vor allem fachlich vorgebildete Datenschutzbeauftragte und Aufsichtsbehörden.

In der einschlägigen Fachliteratur wird bis zur Entwicklung einer eigenen Praxis unter der DSGVO bisweilen die Orientierung an der Praxis anderer Länder mit bereits existierenden Regelungen oder an für andere Bereiche bestehende Leitfäden wie dem „Standard-Datenschutzmodell" der Datenschutzbeauftragten von Bund und Ländern (verfügbar unter https://datenschutzzentrum.de/uploads/SDM-Methode_V_1_0.pdf) angeraten. Abzuwarten bleiben die nach Art. 35 Abs. 4 u. Abs. 5 DSGVO möglichen Positiv- und Negativlisten der Aufsichtsbehörden: Für bestimmte Verarbeitungsprozesse kann mithilfe dieses Instruments eine Folgenabschätzung immer verpflichtend beziehungsweise dauerhaft entbehrlich werden. Einige Beispiele finden Sie in der vorangestellten Literaturliste dieses Abschnitts. Diese könnten bei der Abgrenzung von Verarbeitungen mit und ohne hohem Risiko für eine höhere Rechtssicherheit sorgen.

cc) Verwendung in der Datenschutzkommunikation

Hier ist es natürlich möglich, die ohnehin aus rechtlicher Sicht obligatorisch zu erstellenden Unterlagen und die darin enthaltenen Informationen als Grundlage für die Ausarbeitung von weitergehenden werbewirksamen Dokumenten wie Privacy Policies zu nutzen.

Der Aufwand für die Verantwortliche Stelle ist durch die Nutzung der vorhandenen Datengrundlage vergleichsweise gering. Die Darstellung des Prozesses einer Risikoabschätzung und der Vorfeldmaßnahmen zum Schutz der Betroffenendaten ist aber in hohem Maße geeignet, das Vertrauen der Kunden und Bürger zu wecken.

Sinnvoll könnte jedoch eine Dosierung der Mitteilung möglicher Risiken sein, um die Verarbeitung nicht zu kritisch erscheinen zu lassen, sowie ein Verzicht auf eine zu detailgetreue Schilderung von spezifischen IT-Risiken sein, um nicht die Gefahr eines hierauf aufbauenden Angriffs auf die IT-Infrastruktur zu schaffen.

2. Übernahme von externen Standards

Man unterscheidet im europäischen Recht wie bisher im deutschen Datenschutzrecht zwischen sog. Verhaltensregeln (Art. 40 DSGVO), bei denen es sich um datenschutzrechtliche Regeln handelt, die von Branchenverbänden oder anderen Vereinigungen entworfen werden und von der Aussichtsbehörde geprüft werden, und sog. Unternehmensregelungen (engl. „Binding Corporate Rules"), die nach Art. 47 DSGVO für die grenzüberschreitende Übermittlung von Daten entworfen und durch die Aufsichtsbehörde genehmigt werden können.

a) Verhaltensregeln („Codes of Conduct") (Art. 40 DSGVO)

„Codes of Conduct" stammen aus dem stark auf Selbstregulierung ausgerichteten Recht der Vereinigten Staaten, haben aber in Teilbereichen Entsprechungen im europäischen und deutschen Recht. Die deutsche Fassung der DSGVO verwendet hierfür den Begriff „Verhaltensregeln".

aa) Verfahren

Zwar kann ein Branchenverband grundsätzlich ohne Beachtung bestimmter Vorgaben Selbstverpflichtungen für seine Mitglieder entwerfen und intern für verbindlich erklären. Die im Datenschutzrecht für Verhaltensregeln vorgesehenen Rechtswirkungen treten aber nur ein, wenn das in Art. 40 DSGVO vorgesehene Verfahren zum Erlass solcher Codes of Conduct eingehalten wird.

Nicht jeder kann danach Verhaltensregeln in Zusammenarbeit mit den Aufsichtsbehörden aufstellen. Art. 40 Abs. 2 u. 5 DSGVO beschränken diese Möglichkeit auf „Verbände und andere Vereinigungen". Branchen- und Berufsverbände werden dadurch unproblematisch erfasst, Konzerne möglicherweise nicht. Die Bedeutung und Größe sind dabei jedenfalls nicht relevant.

Die Genehmigung wird grundsätzlich nach 40 Abs. 5 DSGVO von der mitgliedstaatlichen Aufsichtsbehörde am Sitz des Antragstellers erteilt. Sollen sich die Regelungen auf Datenverarbeitungen in mehreren Mitgliedsstaaten der EU beziehen, so muss die mitgliedstaatliche Aufsichtsbehörde zusätzlich eine Genehmigung des Europäischen Datenausschusses einholen (40 Abs. 7 DSGVO).

Werden die Verhaltensregeln von der Aufsichtsbehörde genehmigt, so sind damit Rechtswirkungen verbunden. An zahlreichen Stellen sind bei der Befolgung eines Code of Conduct Erleichterungen für den Nachweis der Einhaltung der Regelungen der DSGVO vorgesehen. Auch wird angenommen, dass die Aufsichtsbehörden durch ihre Genehmigung zumindest bei präzisen Regelungen später einer gewissen Bindung an die dort getroffenen Auslegungen unterliegen. Praktisch dürfte dies durch die Kommunikation während der Erstellung solcher Verhaltensregeln noch viel stärker der Fall sein.

Ohne eine weitere Umsetzung innerhalb des Verbandes haben Codes of Conduct jedoch überhaupt keine weitere Rechtsqualität und können insbesondere keine Ansprüche für Betroffene begründen. Je nach Umsetzung können diese aber zumindest dadurch verbandsintern Verbindlichkeit erlangen, dass sich die Mitglieder diesen durch Beitritt oder Zustimmung freiwillig unterwerfen. Selbst diese beschränkte Verbindlichkeit ist aber keinesfalls unumstritten. Hierzu müsste von einem erhöhten Interesse des Verbandes an der Einhaltung der datenschutzbezogenen Verhaltensregeln auszugehen sein, was sich nicht für jede Branche pauschal bejahen lässt.

bb) Möglicher Inhalt

Codes of Conduct enthalten meist Erklärungen über die Werte und Geschäftspraktiken. Sie zeichnen ein Bild des Unternehmens und können zu den angestrebten Datenschutzstandards Stellung beziehen. Sinn und Zweck solcher Verhaltensregeln ist die Anpassung der oft abstrakten und generellen gesetzlichen Vorgaben an die speziellen Bedürfnisse einer Branche. Die Überprüfung durch die Aufsichtsbehörden führt dabei zwar nicht zu

einer Verbindlichkeit der Regelungen, wohl aber zu einer gewissen Orientierung an die dort vorgenommenen Auslegungen. Genaue Mindestinhalte sind für die Verhaltensregeln aber in der DSGVO nicht vorgegeben.

Mögliche Inhalte sind in Art. 40 Abs. 2 lit. a–k DSGVO beispielhaft aufgezählt. Im Wesentlichen steht die Konkretisierung von Generalklauseln und Anpassung an verarbeitungsbezogene Besonderheiten der jeweiligen Branche im Vordergrund.

cc) Verwendung in der Datenschutzkommunikation

Die Möglichkeiten zur Aufstellung solcher Verhaltensregeln werden zwar vereinzelt genutzt, von einer weiten Verbreitung lässt sich aber aufgrund der überschaubaren Zahl von Fällen bisher kaum sprechen. Durch die detaillierteren Regeln der DSGVO zum Genehmigungsverfahren und auch durch die genauere Betrachtung der Rechtsfolgen wird dieses Instrument der „regulierten Selbstregulierung" aber für die Zukunft deutlich gestärkt.

Eine Veröffentlichung und Kommunikation obliegt nicht nur den diesen Verhaltensregeln unterworfenen Stellen. Nach Art. 40 Abs. 6 DSGVO sind diese schon von den Aufsichtsbehörden in ein Verzeichnis aufzunehmen und zu veröffentlichen.

Ein Verweis auf dieses Verzeichnis kann innerhalb der eigenen Kommunikation mit der Öffentlichkeit positiv genutzt werden, indem die Prüfung durch die Aufsichtsbehörde herausgestellt wird. Dabei steht es im Belieben des einzelnen Verarbeiters, ob er die Existenz eines Code of Conduct und dessen Inhalte innerhalb der eigenen Werbestrategie weiter ausnutzt und durch explizite Hinweise darauf zusätzliche positive Wettbewerbseffekte generiert.

Und auch wenn aus Sicht des jeweiligen Verarbeiters branchenweite Übereinkünfte keine individuellen positiven Vorteile in der Datenschutzkommunikation generieren, dienen sie aber zumindest einer Abgrenzung von „schwarzen Schafen" in einem möglicherweise von den Verbrauchern grundsätzlich als eher wenig vertrauenswürdig eingestuften Sektors.

Langfristig kann durch Codes of Conduct, neben der Schaffung von mehr Rechtssicherheit für die beteiligten Verarbeiter, das Vertrauen des Verbrauchers in die Gesamtbranche gesteigert werden.

Schließlich sollte auch der Aspekt der Kommunikation mit der Aufsichtsbehörde während des Genehmigungsprozesses nicht vernachlässigt werden. Hier besteht die Möglichkeit einer sehr gezielten Lobby-Arbeit, um die Generalklauseln der DSGVO für die Gegebenheiten in der eigenen Branche handhabbar zu machen.

b) Binding Corporate Rules

Binding Corporate Rules oder „verbindliche interne Datenschutzvorschriften" unterscheiden sich in diversen zentralen Punkten von Codes of Conduct. Für diese enthält Art. 4 Nr. 20 DSGVO sogar eine Definition.

Anders als Codes of Conduct werden Binding Corporate Rules jeweils nur für die interne Datenweitergabe in einem Unternehmen oder einer Unternehmensgruppe erlassen. Auch der Anwendungsbereich ist deutlich begrenzter: Geregelt wird hier lediglich der Datentransfer in Länder außerhalb der EU (sog. Drittländer). Sie sollen die Daten innerhalb des Unternehmens grenzüberschreitend verfügbar machen können.

aa) Verfahren

Die verbindlichen internen Vorschriften sind ebenfalls von der zuständigen Aufsichtsbehörde zu genehmigen. Bei Niederlassungen in mehreren Mitgliedsstaaten muss, wie bei den Codes of Conduct beschrieben, ein Kohärenzverfahren nach Art. 63 DSGVO stattfinden.

Zentrale Genehmigungsvoraussetzung ist nach Art. 47 Abs. 1 lit. a DSGVO die rechtliche Verbindlichkeit der Datenschutzvorschriften innerhalb des Unternehmens oder Unternehmensgruppe. Wie dies genau zu erreichen ist, hängt unter anderem von den Rechtsformen der beteiligten Unternehmensteile ab und kann hier nicht im Detail dargestellt werden. Vertragliche Verpflichtungen untereinander werden aber als genügend angesehen. Andere Konstruktionen sind denkbar, sofern sie eben zu einer rechtlichen Verbindlichkeit führen. Eine genauere Regelung des Verfahrens kann in Zukunft nach Art. 47 Abs. 3 DSGVO ggf. noch durch die Europäische Kommission erfolgen.

bb) Inhaltliche Anforderungen

Die DSGVO enthält inhaltliche Vorgaben für die Aufstellung von Binding Corporate Rules. Eine Genehmigungsvoraussetzung ist die Aufnahme von durchsetzbaren Rechten für die Betroffenen (Art. 40 Abs. 1 lit. b DSGVO). Die Regelungen sollen also nicht nur innerhalb des Unternehmens verbindlich sein, sondern auch nach außen Wirkungen entfalten.

Daneben enthält Art. 40 Abs. 2 DSGVO einen umfangreichen Katalog an Mindestangaben, die bei der Erstellung abzuarbeiten sind.

cc) Verwendung in der Datenschutzkommunikation

Das Thema der Übermittlung von Daten in Drittländer hat in den letzten Jahren eine enorme mediale Aufmerksamkeit erfahren. Gerade die Übermittlung von Daten in die USA wurde als skandalträchtiges Thema im Rahmen der Offenlegung dortiger Geheimdienst-Praktiken breit diskutiert. Das Schlagwort „Safe Harbor“, welches die damaligen Regelungen für solche Übermittlungen zusammenfasste, war medial über Monate präsent. Auch das ebenfalls häufig kritisierte Nachfolgeabkommen „Privacy Shield“ ist in aller Munde.

Gerade bei solchen Übermittlungsprozessen gilt es also, das möglicherweise erschütterte Vertrauen der Betroffenen zurückzugewinnen. Die Aufstellung und Genehmigung von Binding Corporate Rules können dabei aber nur die ersten Schritte sein und schaffen nur die rechtliche wie kommunikative Grundlage.

Eine transparente Offenlegung der Übermittlung kann hier dann zusätzliches Vertrauen schaffen. Letztendlich liegt hier durch die umfangreichen Mindestinhalte wieder eine gute Informationsgrundlage vor, auf die in der weiteren öffentlichen Kommunikation aufgebaut werden kann. Die Genehmigung durch die Aufsichtsbehörde wirkt hier als zusätzliches Vertrauensmerkmal.

Durch die individuelle Regelung innerhalb des Unternehmens bzw. der Unternehmensgruppe besteht hier die Möglichkeit, sich positiv von anderen Mitbewerbern abzuheben und eine durch oben geschilderte Skandale sensibilisierte Gruppe von Betroffenen für sich zu gewinnen.

c) Zertifikate und Datenschutz-Siegel

Stiftung Datenschutz, Hintergrundinformationen zu Datenschutzgütesiegeln, abrufbar unter:
https://stiftungdatenschutz.org/aufgaben/zertifikate-uebersicht/hintergrund-guetesiegel/

Neben den oben beschriebenen häufig langen Dokumenten können auch Zertifizierungen und Datenschutzsiegel ein Mittel der Kommunikation sein. Sie erlauben es den Betroffenen auf einen Blick die Übereinstimmung eines Angebotes mit den Kriterien des Siegelanbieters zu prüfen und somit Vertrauen zu erwecken. Hierfür muss der Zertifizierung allerdings ein transparenter und umfangreicher Prüfungsprozess vorausgegangen sein, und die betreffende Zertifizierung bzw. das Siegel muss unter den Betroffenen bekannt sein.

Die Stiftung Datenschutz bietet auf ihrer Internetseite einen umfangreichen Überblick zu momentan 32 Anbietern von Zertifizierungen und Gütesiegeln an, inklusive einer Auflistung der Prüfungsvoraussetzungen (abrufbar unter https://stiftungdatenschutz.org/aufgaben/zertifikate-uebersicht/).

Wird der Anbieter des Zertifikats vom Verbraucher als vertrauenswürdig eingestuft, kann der Datenverarbeiter an diesem Ruf durch Verwendung des Zertifikats im Rahmen seiner Kommunikation teilhaben.

Erstmals kommen den Zertifizierungen und Gütesiegeln mit der DSGVO rechtliche Wirkungen zu. Die Zertifizierungen sind hierfür nach Art. 42 Abs. 5 DSGVO durch eine Aufsichtsbehörde zu genehmigen. Hieraus wird dann eine europaweite und zu veröffentlichende Liste durch den Europäischen Datenschutzausschuss zu erstellen sein (Art. 42 Abs. 8 DSGVO).

aa) Verfahren

Neu sind zahlreiche formelle Vorgaben für die Zertifizierung. Diese muss für das Eintreten rechtlicher Wirkungen nicht nur in oben beschriebener Weise staatlich anerkannt sein, sondern spätestens alle drei Jahre wiederholt werden (Art. 42 Abs. 7 DSGVO). Art. 42 Abs. 6 DSGVO stellt klar, dass eine umfangreiche Mitwirkung des zu zertifizierenden Verantwortlichen erforderlich ist. Praktisch ist die Durchführung eines Zertifizierungsverfahrens anders gar nicht denkbar. Auch der Zeitraum dürfte die der obigen Übersicht (c.) zu entnehmenden etablierten Anbieter vor keine größeren Umsetzungsprobleme stellen.

bb) Inhaltliche Anforderungen

Die unter der DSGVO genehmigten Zertifikate belegen aus inhaltlicher Sicht gem. Art. 42 Abs. 1 S. 1 DSGVO die Einhaltung der Vorgaben des europäischen Datenschutzrechts. Eine darüber hinaus gehende Prüfung höherer Datenschutzstandards wird in diesem Verfahren bisher nicht für möglich gehalten. Letzten Endes belegt ein genehmigtes Zertifikat somit nur die Einhaltung der ohnehin zu beachtenden rechtlichen Mindestvorgaben. Die Zukunft der oben genannten Zertifikate bleibt abzuwarten. Freilich ist es nicht undenkbar, dass über die unter der DSGVO vorgeschriebene Zertifizierung hinaus andere Zertifikate am Markt so etabliert werden, dass auch ohne eine Genehmigung Wettbewerbseffekte und gestärktes Vertrauen entstehen können.

cc) Verwendung in der Datenschutzkommunikation

Die Zertifizierung kann, wie auch andere Formen der unabhängigen Bewertung von Datenschutz, Teil der Kommunikationsstrategie sein. Dem Betroffenen können diese als Anhaltspunkt für ihr Nutzungsverhalten und ihren datenschutzbezogenen Selbstschutz dienen. Sie geben schnell und auf einen Blick Orientierung und eignen sich damit aus Sicht der Verantwortlichen Stelle als Werbewerkzeug und können Nachfrage und damit Wettbewerbsvorteile generieren. Auf einen Blick wird die Einhaltung bestimmter Standards visuell für den Betroffenen dargestellt. Abhängig von den konkreten Anforderungen an die Verantwortliche Stelle kommt eine Kombination mit den weiteren vorgestellten Instrumenten in Betracht.

3. Freiwillige allgemeine Datenschutzkommunikation (Privacy Policies)

***Jansen**, in: Moos (Hrsg.), Datennutzungs- und Datenschutzverträge – Muster, Klauseln, Erläuterungen, Otto Schmidt-Verlag 2014, S. 959*
***Schröder**, Die Haftung für Verstöße gegen Privacy Policies und Codes of Conduct nach US-amerikanischem und deutschem Recht, Nomos 2007*

Der Begriff Privacy Policies wird auch in Deutschland zunehmend verwendet. Hierbei gilt es aber zu beachten, dass es sich dabei anders als in den Vereinigten Staaten von Amerika nicht um einen feststehenden Rechtsbegriff handelt.

Dies macht die Privacy Policies einerseits zu einem flexiblen Kommunikationsinstrument, da keine engen rechtlichen Begrenzungen vorgegeben sind. Andererseits können diese aber je nach Gestaltung auch vertragliche Pflichten mit sich bringen, die vom Informierenden im Kern gar nicht beabsichtigt waren. Je nach Gestaltung können Privacy Policies aus rechtlicher Sicht als (un)verbindliche Selbstverpflichtung, als AGB oder gar als selbstständiges Garantieversprechen bewertet werden. Häufig wird der Begriff aber einfach synonym zum Begriff der Datenschutzerklärung verwendet. Es wird dann unter der Überschrift lediglich den unten dargestellten gesetzlichen Informationspflichten nachgekommen.

Nach geltendem Datenschutzrecht gibt es keine Pflicht zu einer öffentlichen „Privacy Policy". Aber gerade weil keine solche Pflicht besteht, kann sich auf diesem Feld von Wettbewerbern abgesetzt und über den gesetzlichen Mindeststandard hinausgegangen werden.

a) Kein formelles Verfahren

Mangels gesetzlicher Regelung gibt es für Privacy Policies an sich und ihre Entstehung keine einheitlichen Verfahrens- und Formvorschriften. Je nach Aufnahme bestimmter verpflichtender Angaben direkt in eine Privacy Policy, können aber die bei den spezifischen Kommunikationsanlässen dargestellten Form- und Verfahrensanforderungen Anwendung finden.

Da sich sowohl Inhalt, als auch Rechtsform der Privacy Policies stark unterscheiden können, sind diese Anforderungen im Einzelfall zu prüfen. Dabei sind jeweils die genauen rechtlichen Bindungswirkungen und möglicherweise entstehenden Ansprüche der Betroffenen kritisch zu würdigen. Eine Bindung wird in den meisten Fällen bei werblichen Privacy Policies gar nicht gewünscht sein und ist deshalb klarstellend möglichst zu vermeiden.

b) Inhaltliche Anforderungen (Werbende Verständlichkeit von Privacy Policies)

***Eichhorn/Schuhmann**, Der Inhalt ist alles, die Form nur Ästhetik?, Zeitschrift für deutsches und internationales Bau- und Vergaberecht (ZfBR), 2014, S. 211 ff. abrufbar unter http://t1p.de/p2xb [Beck-online, kostenpflichtig]*

Soll eine umfassende Privacy Policy neben werberelevanten Texten auch rechtliche Informationspflichten erfüllen, so ist im Detail auf die unten (III.) folgenden Voraussetzungen zu spezifischen Kommunikationsanlässen zu verweisen. Es gelten dann die in der DSGVO aufgeführten Prinzipien, insbesondere die Grundanforderung des Art. 12 Abs. 1 DSGVO nach einer klaren und einfachen Sprache.

Unabhängig von einer rechtlichen Verpflichtung ergeben sich ähnliche Anforderungen für einen werbewirksamen Text hier schon aus kommunikationspraktischer Sicht. Die Stiftung Warentest hat in einem Test von Datenschutzerklärungen diesbezüglich diverse Problemfelder aufgezeigt (test 3/2016, S. 57 ff.). So waren die untersuchten Erklärungen bis zu 45 Seiten lang. Dennoch fehlte es zum Teil immer noch an einer Erfüllung der rechtlichen Pflichten. Daneben ist eine Werbewirkung bei diesem Umfang wohl kaum zu erwarten. Dabei zeigen bereits verschiedene Studien, dass sich die Lesbarkeit und das Verständnis von Datenschutzerklärungen und anderer Rechtstexte insgesamt positiv auf das Bild des Verarbeiters und das Vertrauen der Betroffenen auswirken können.

aa) Kommunikation durch Layout

Eine Orientierung an der DSGVO ist hier geboten. Art. 12 Abs. 7 DSGVO verlangt eine leicht wahrnehmbare, verständliche und klar nachvollziehbare Form. Dies verlangt eine übersichtliche Gliederung des Dokumentes und die Verwendung geeigneter Hervorhebungen, um die Übersichtlichkeit zu erhöhen. Beitragen hierzu können ein großer Zeilenabstand, Einrückungen und Zwischenüberschriften.

Datenschutzerklärungen können insbesondere im Internet interaktiv gestaltet werden und durch die Verwendung von Hyperlinks in mehreren Ebenen aufgebaut werden. Ausgangspunkt ist dann ein kurz gehaltenes Überblicksdokument, das in den weiteren Schritten mit einer umfangreichen Privacy Policy verknüpft wird. Ein zusätzlicher Klick leitet den Betroffenen zu weiterführenden Informationen. Solche klickbaren Verweise sind dabei textlichen Verweisen vorzuziehen. Zur Visualisierung können zusätzlich Piktogramme beitragen. Der Verweis auf erworbene Datenschutzsiegel und Zertifizierungen ermöglicht dem Kunden eine weitere Orientierung.

bb) Besonderheiten der Mensch-Maschine-Kommunikation

Gerade bei der Verwendung digitaler Informationssysteme sind die Grundsätze der Mensch-Maschine-Interaktion zu beachten. Orientierung kann hier die ISO-Norm ISO 9241-110 geben. Diese stellt Dialoggrundsätze für interaktive Systeme auf. Der Nutzer muss die zu vermittelnden Informationen vollständig, korrekt und insbesondere mit vertretbarem Aufwand erhalten können. Gerade aufgrund der beschriebenen rationalen Apathie in Bezug auf Datenschutzthemen müssen hier die Hemmschwellen bei der Bedienung möglichst klein gehalten werden.

Auch die Navigation auf der angebotenen Seite muss benutzerfreundlich ausgestaltet sein. Der Benutzer muss sich jederzeit orientieren können und insbesondere wissen, wie er eine bestimmte Seite erreicht hat und auch wieder zurück zu den zuvor gelesenen Inhalten gelangt. Dies verlangt von dem verwendeten System eine hohe Toleranz bezüglich aller denkbaren Bedienungsfehler.

Genau wie der Text muss das Informationssystem auch den Erwartungen der Zielgruppe angepasst werden. Je nach Endgerät ist hier auf verbreitete Üblichkeiten in der Bedienung Rücksicht zu nehmen und sich diesen anzupassen.

cc) Kommunikation auf der Textebene

***Europäische Kommission**, Klar und deutlich schreiben, http://t1p.de/d3cq [Europ. Kommission, kostenfrei]*

Auf der Textebene sollte auf eine klare und einfache Sprache geachtet werden. Wenn die Stiftung Warentest in Datenschutzerklärungen auf Sätze mit bis zu 130 Wörtern gestoßen ist, wird man diesem Erfordernis in der Praxis zum Teil nicht einmal annähernd gerecht. Eine gute Lesbarkeit erhöht nachweislich das Textverständnis. Zu vermeiden sind hierbei insbesondere lange und komplexe Satzkonstruktionen. Gerade Aufzählungen lassen sich zur besseren Lesbarkeit häufig geeigneter in Bullet-Points darstellen. Ergänzend können Tabellen zum Einsatz kommen.

Eine direkte Ansprache wird dabei von den Betroffenen als persönlicher empfunden und ist somit oft vorzugswürdig. Allerdings hängt dies auch von der jeweiligen Dienstleistung, dem jeweiligen Produkt und der jeweiligen Verantwortlichen Stelle ab.

Insbesondere bei rechtlichen und technischen Ausführungen besteht immer die Gefahr einer durch „Fachchinesisch“ oder „Juristendeutsch“ für die angesprochene Zielgruppe völlig ungeeigneten Ansprache. Im englischen Sprachraum hat sich insbesondere bei Rechtstexten aus dieser Problemlage mit dem „Plain Language Movement“ eine Gegenbewegung etabliert. Die Bedeutung für den deutschen Sprachraum hält sich hier aber bisher noch in Grenzen. Ähnliche Prinzipien werden aber im Rahmen des Draftings und der Legistik auch hierzulande vertreten. So hat beispielsweise das österreichische Kanzleramt schon 1990 eine legistische Richtlinie zur Verbesserung der Rechtssprache herausgegeben (Bundeskanzleramt Österreich, Handbuch der Rechtssetzungstechnik, Teil 1: Legistische Richtlinien, Wien 1990, verfügbar unter http://archiv.bundeskanzleramt.at/DocView.axd?CobId=1656). Ähnliche Bestrebungen gibt es ausweislich des oben angeführten Dokuments

auf Ebene der Europäischen Kommission. Klarheit, Präzision, Widerspruchsfreiheit, Lesbarkeit und Verständlichkeit sind insbesondere bei Gesetzen schon aus rechtsstaatlicher Sicht geboten. Dies lässt sich ohne weiteres auf Datenschutztexte übertragen. Weitere in der Richtlinie angesprochene Punkte sind der Verzicht auf Schachtelsätze, die Beschränkung eines Satzes auf möglichst eine zentrale Aussage und wie bereits oben erwähnt die Beschränkung der Satzlänge. Als Anhaltspunkt wird dort von einer Maximallänge von 20 Wörtern ausgegangen.

Im Feld der Kommunikationsoptimierung gibt es zusätzlich ein großes Angebot an Werbeagenturen und spezialisierten Dienstleistern, die über das nötige Knowhow verfügen, um insbesondere kleinen Unternehmen und Behörden ohne eigene PR-Abteilung bei der Erstellung verständlicher Texte zu unterstützen.

dd) Kommunikation auf der Inhaltsebene

Freilich ist neben den oben geschilderten Äußerlichkeiten auch inhaltlich darauf zu achten, dass die Privacy Policies nicht nur dazu dienen dürfen, der Verantwortlichen Stelle möglichst viele Daten zu verschaffen und Datenschutzprobleme zu relativieren. Auf diese Weise kann selbst ein gut formuliertes Dokument kein dauerhaftes Vertrauen der Betroffenen wecken. Zu weite, pauschale Ermächtigungen sind zudem auch rechtlich problematisch, wie die Kontrolle der Datenschutzbestimmungen von Google durch die Artikel 29-Datenschutzgruppe im Jahr 2012 deutlich machte. Insgesamt zeigt sich, dass die Einhaltung guter kommunikativer Standards häufig ohnehin Rechtspflicht ist.

c) Verwendung in der Datenschutzkommunikation

***Lange-Hausstein**, Automatisierte Vertragsfreiheit, LTO [Legal Tribune Online], 28.12.2016, abrufbar unter http://t1p.de/0l4d [Legal Tribune Online, kostenfrei]*

***Steinlechner**, Verbraucherschützer: IT-Branche schadet sich mit starren AGB-Vorgaben, golem IT-News, 29.12.2016, abrufbar unter http://t1p.de/z901 [golem IT-News, kostenfrei]*

***Schätzle**, Smarte Assistenzsysteme als Entscheidungsersatz, Telemedicus Sommerkonferenz 2015, abrufbar unter http://t1p.de/m2xh [PinG Blog, kostenfrei]*

Anknüpfend an die obigen Darstellungen zur Nutzung der interaktiven Gestaltungsmöglichkeiten könnte zur Umsetzung auch an ein umfangreiches Privacy Assistenzsystem gedacht werden. Rechtlich verpflichtend ist dies freilich nicht. Gerade deswegen könnte sich ein Verarbeiter aber hier deutlich positiv von der Konkurrenz oder dem bloßen Pflichtprogramm abheben.

Erste Ansätze, die sich aber in der Praxis bisher leider kaum durchgesetzt haben, lieferte hierfür auf Protokoll-Ebene der p3p-Standard. Datenschutzerklärungen sollten mit dieser Hilfe durch die Bereitstellung von maschinenlesbaren Informationen automatisch durch den Browser oder ein Plug-In mit den Datenschutzvorgaben des Nutzers abgeglichen werden.

Konsequent weitergedacht könnte durch den Einsatz von geeigneten Algorithmen an dieser Stelle über die Voreinstellungen des Nutzers hinaus anhand des bisherigen Zustimmungsverhaltens eine Zustimmung oder Ablehnung der Bedingungen ermittelt und diesem präsentiert werden. Durch die Zuhilfenahme solcher technischen Systeme kann der „information overflow“ wirkungsvoll eingedämmt werden.

Wie in vielen anderen Bereichen schon üblich, wäre auch ein auf Userbewertungen basiertes System denkbar, das Seiten aufgrund ihrer Verpflichtung zu bestimmten Datenschutzprinzipien für vertrauenswürdig erklärt.

Solche Lösungen von durchdachten Privacy Assistenz-Systemen können bei geeigneter technischer Umsetzung eine höhere Flexibilität ermöglichen: Zur Zeit kann der dargestellte Datenschutzstandard eines Unter-

nehmens entweder bestätigt oder abgelehnt werden. Es erscheint aber durchaus denkbar, dass ein durch die Ablehnung verlorener Kunde durch eine flexiblere Gestaltung davon überzeugt werden kann, das angebotene Produkt doch in Anspruch zu nehmen. Dies kann beispielsweise schon durch die Abwahlmöglichkeit von in der Gesamtschau zweitrangigen Verarbeitungen realisiert werden. Letztendlich könnten hier brachliegende Potentiale genutzt werden.

Sicher betritt man als Verarbeiter zum jetzigen Zeitpunkt mit solchen Ansätzen noch Neuland. Anderseits ermöglicht gerade die Stellung als Pionier in diesem Bereich Vorteile gegenüber denjenigen, die hier erst später auf den Zug aufspringen.

III. Spezifische Kommunikationsanlässe

Während also eine allgemeine Datenschutzkommunikation an die Öffentlichkeit in Form von Privacy Policies o.ä. nützlich sein kann, aber nicht vorgeschrieben ist, ist der Betroffene im Kontext konkreter Datenverarbeitungen verpflichtend nach Maßgabe des Datenschutzrechts zu informieren. Hier bestehen detaillierte Vorgaben, die aber nicht (nur) nach den Buchstaben des Gesetzes erfüllt werden müssen, sondern denen noch ein kommunikativer Mehrwert mitgegeben werden kann.

1. Gesetzliche Informierungspflichten des Verantwortlichen gegenüber dem Betroffenen

Zur Verringerung des Informationsgefälles zwischen Betroffenem und der Verantwortlichen Stelle sieht das Datenschutzrecht zeitlich dreifach gestufte Informierungen vor:

Im Regelfall soll der Betroffene vor oder bei der Erhebung der Daten bereits unterrichtet werden. Dies ist im Falle der Einwilligung (a.) und bei der sog. Direkterhebung (b.) unproblematisch umsetzbar, da ohnehin ein Kontakt und eine Kommunikation besteht. Besteht kein direkter Kontakt, wird zum Teil auf die Kenntnisnahme

einer Kennzeichnung (b.cc)) gesetzt. Wo dies nicht der Fall bzw. nicht praktikabel ist, sieht das Gesetz die nachgängige Benachrichtigung (c.) vor. Insbesondere ist dies dort der Fall, wo Daten nicht vom Betroffenen selbst, sondern aus anderer Quelle erhoben werden. Wenn der Betroffene weitere Einzelheiten wissen will, die initiale Information bei ihm nicht (mehr) vorhanden ist oder (ausnahmsweise) entbehrlich war, besitzt er ein Auskunftsrecht (d.).

a) Information für Einwilligung

***Pollmann/Kipker**, Informierte Einwilligung in der Online-Welt, DuD [Datenschutz und Datensicherheit] 2016, S. 378 ff., abrufbar unter http://t1p.de/mrcm [Springer Link, kostenpflichtig]*

Neben der Verarbeitung von Daten auf Grundlage einer gesetzlichen Erlaubnis besteht die Möglichkeit, darüber hinaus Daten mit Einwilligung des Betroffenen zu verarbeiten.

Hier „lohnt" sich die Kommunikation über die Erfüllung der rechtlichen Pflichten hinaus. So kann sich der Bearbeiter nämlich die Erlaubnis für die Verarbeitung weiterer Daten und in zusätzlichen Kontexten erschließen, die er sonst nicht verarbeiten dürfte.

Für die Kommunikation mit dem Betroffenen im Hinblick auf seine Einwilligung sind daher zwei Aspekte zu beachten: Zum einen enthält die DSGVO diverse rechtliche Vorgaben, die für die Wirksamkeit der Einwilligung entscheidend sind und die umfangreiche Anforderungen an Art und Qualität der Kommunikation stellen. Zum anderen muss die Kommunikation auch unabhängig von diesen rechtlichen Vorgaben so erfolgen, dass sie beim Betroffenen das nötige Vertrauen weckt, um in eine Verarbeitung einzuwilligen. Ursprünglich als Instrument der informationellen Selbstbestimmung gedacht, wird die Einwilligung so zunehmend als Instrument zur Kommerzialisierung der eigenen persönlichen Daten (Daten im „Tausch" gegen Leistung) genutzt.

aa) Verfahren und Form der Einwilligung

Der Betroffene ist auf die Widerruflichkeit dieser Einwilligung sowie auf sein Widerspruchsrecht hinzuweisen. Diese Informationen müssen dem Nutzer jederzeit zum Abruf zur Verfügung stehen.

Art. 4 Nr. 11 DSGVO enthält eine Definition der Einwilligung. Neben einer ausdrücklichen Erklärung werden hier auch eindeutige, bestätigende Handlungen zugelassen. Ausgeschlossen soll hier angesichts des Erwägungsgrundes 32 die (nur) komplette Untätigkeit sein. So wird explizit erwähnt, dass Stillschweigen, vorangekreuzte Kästchen oder Untätigkeit keine Einwilligung darstellen können. Möglich wären demnach:

- die Einwilligung durch Ankreuzen eines Formularkästchens per Mausklick
- die Einwilligung per Email,
- die mündliche Einwilligung,
- sowie nach Erwägungsgrund 32 auch die Einwilligung per Voreinstellungen im Browser, z.B. die Voreinstellung einer bestimmten Cookie-Policy.

Auch der Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation (EU-Privacy-VO) sieht Einwilligungen in Form von Softwareeinstellungen ausdrücklich vor (vgl. den gegenwärtigen Entwurf des Art. 9 Abs. 2 EU-Privacy-VO; die Trilog-Verhandlungen zwischen Europäischer Kommission, dem Rat der Europäischen Union und dem Europäischen Parlament stehen noch aus, sodass sich der Entwurf und insb. die Artikelzählung noch ändern kann). Im Hinblick auf die weitgehend formfreie und insbesondere auch mündlich mögliche Einwilligung ist aber auf Art. 7 Abs. 1 DSGVO hinzuweisen: Im Zweifel muss die Verantwortliche Stelle das Vorliegen einer Einwilligung beweisen können. Die elektronische oder schriftliche Form sollte aus Dokumentationsgesichtspunkten also den Regelfall darstellen.

Daneben ist sicherzustellen, dass die Einwilligung freiwillig, d.h. ohne Zwang, erfolgt. Dies adressiert die DSGVO insbesondere im Hinblick auf ein klares Ungleichgewicht der Vertragsparteien (ErwGr. 43 zur DSGVO) und bezüglich einer unnötigen Koppelung von Leistung und Einwilligung (Art. 7 Abs. 4 DSGVO). In der Zusammenschau dieser beiden Regelungen ist sicher davon auszugehen, dass unter Geltung der DSGVO nicht jede Koppelung von Leistung an eine nicht zwingend zur Erfüllung erforderliche Einwilligung gemeint sein kann. In der englischen Fassung heißt es: „Consent is presumed not to be freely given…", was eher mit „Die Einwilligung ist mutmaßlich nicht freiwillig erteilt…" zu übersetzen gewesen wäre. Eine enge Auslegung des Koppelungsverbots wäre mit Blick auf die praktische Kommerzialisierung der Einwilligung im „Tausch" gegen eine Dienstleistung kaum sachgerecht umsetzbar. Auch die deutschen Aufsichtsbehörden legen das Koppelungsverbot daher eng aus, weil sie keine Bedenken gegen die werbliche Nutzung der Daten durch den Verarbeiter haben, wenn z.B. hierfür eine E-Mail-Dienst unentgeltlich angeboten wird. Direkte Auswirkungen dieser Regelung dürften sich daher aller Voraussicht nach besonders auf Monopol-Anbieter in bestimmten Märkten beschränken.

bb) Informiertheit als inhaltliche Anforderung

Damit ein Betroffener eine Einwilligung bewusst abgeben kann, muss er sich über die Datenverarbeitung, in die er einwilligt, im Klaren sein. Dies stellt eine weitere Ausprägung des Transparenzgrundsatzes dar. Das Datenschutzrecht fordert nicht nur äußerlich einen entsprechenden rechtlichen Text oder eine vorhandene technische Beschreibung, sondern ein tatsächliches Verständnis beim Betroffenen. Juristen sprechen insoweit von der „Maßgeblichkeit des individuellen Empfängerhorizonts" oder teils von einem nutzerzentrierten Verständnis. Es kommt also darauf an, dass der konkret einwilligende Betroffene informiert ist, nicht allein aber, dass die Einwilligungserklärung als solche informativ ist. Dabei ist gerade nicht nur der Inhalt, sondern eben auch die Qualität, der einfache Zugang, die Verständlichkeit der Informationen zu berücksichtigen.

cc) Besonderheiten bei der Einwilligung von Kindern

***UNICEF**, UN Convention on the Rights of the Child in Child Friendly Language, http://t1p.de/7072 [UNICEF, kostenfrei]*

Die DSGVO stellt erstmals spezifische Anforderungen an die Einwilligung von Kindern, wenn auch nur im Kontext von Onlinediensten. Diese werden damit im Datenschutzkontext als besonders gefährdete Zielgruppe herausgehoben.

Dabei gelten die Besonderheiten laut Art. 8 Abs. 1 DSGVO nur, wenn ein Angebot von Diensten der Informationsgesellschaft einem Kind direkt gemacht wird. Dies ist als Beschränkung auf solche Dienste zu verstehen, deren Zielgruppe explizit Kinder sind. Nicht jede Seite, die möglicherweise und unter anderem von Kindern genutzt wird, muss also den Vorgaben genügen.

Wer „Kind" ist, wird von der DSGVO nicht abschließend definiert. Personen, die das sechzehnte Lebensjahr vollendet haben, gelten in jedem Fall als einwilligungsfähig. Ob in einigen Ländern von der Möglichkeit Gebrauch gemacht wird, diese Grenze bis zur Vollendung des dreizehnten Lebensjahres abzusenken, bleibt abzuwarten. Im deutschen Recht wurde hiervon nicht Gebrauch gemacht. Die Umsetzungen vieler anderer EU-Staaten lassen auf sich warten. Hier könnten wiederum komplizierte Folgeprobleme bezüglich der Bestimmung des anwendbaren mitgliedstaatlichen Rechts entstehen, die dem eigentlichen Harmonisierungsziel der DSGVO widersprechen.

Ist der Betroffene nach diesen Regelungen nicht selbst zur Einwilligung fähig, so muss sich die Verantwortliche Stelle nach Art. 8 Abs. 2 DSGVO vergewissern, dass die Einwilligung durch die Eltern oder mit deren Zustimmung erteilt wurde. Hier sind angemessene Anstrengungen im Rahmen des technisch Möglichen zu unternehmen.

Hinzuweisen ist hier noch auf eine in Erwägungsgrund 38 angesprochene spezielle Bereichsausnahme: Präventions- und Beratungsdienste sollen Kindern weiterhin ohne die Mitwirkung und damit das Wissen der Eltern zur Verfügung gestellt werden können.

Richtet sich ein Angebot nur oder hauptsächlich an Kinder, so ergibt sich auch schon aus den sonstigen allgemeinen Kommunikationsvorschriften der DSGVO, dass die Sprache der rechtlich verlangten Mitteilungen konsumentengerecht, sprich also hier kindgerecht sein muss. Orientierung kann die oben angeführte Handreichung der UNICEF in kindgerechter Sprache bieten.

b) Unterrichtung bei der Erhebung

Das Recht kennt bisher an verschiedenen Stellen Unterrichtungspflichten zum Zeitpunkt der Erhebung von persönlichen Daten (so auch ErwGr. 61 DSGVO). Die Grundsätze einer fairen und transparenten Verarbeitung machen es erforderlich, dass der Betroffene über die Existenz des Verarbeitungsvorgangs und seine Zwecke unterrichtet wird (ErwGr. 60 DSGVO).

aa) Verfahren und Form

Mit Art. 13 DSGVO wird ein umfangreicher Katalog von Informationen zur rechtlichen Pflicht. Auch die Beschreibung der Vorgänge in einer einfachen und deskriptiven Sprache könnte zu wesentlich längeren Texten führen. Ob diese Menge an Informationen in der Praxis tatsächlich zu einer besseren und informierten Entscheidung des Betroffenen führt, darf im Hinblick auf das Phänomen des „Information Overkill“ bezweifelt werden. Es führt an einer Einhaltung der gesetzlichen Pflichten dennoch kein Weg vorbei. Es muss ein Mittelweg zwischen der effizienten und verständlichen Informierung einerseits und der Erfüllung der inhaltlichen Mindestanforderungen auf der anderen Seite gefunden werden.

Ergänzend sieht die DSGVO in Art. 12 Abs. 7 noch die Verwendung von Piktogrammen vor, die wiederum zu einer erhöhten Übersichtlichkeit beitragen sollen. Im Idealfall seien diese dazu noch leicht wahrnehmbar, verständlich und klar nachvollziehbar. Eine Erstellung solcher Symbole soll dem Europäischen Datenschutzausschuss übertragen werden.

bb) Inhaltliche Anforderungen

Die inhaltlichen Anforderungen für die Unterrichtung des Betroffenen bei Erhebung personenbezogener Daten enthält Art. 13 DSGVO. Ähnlichkeiten lassen sich zu den bisherigen Regelungen in §§ 5, 13 TMG erkennen. Auch hier sind nicht die erfassten persönlichen Daten selbst mitzuteilen. Ein Blick auf die entsprechende Norm, die in gedruckter Fassung beinahe 2 DIN A4-Seiten füllt, verschafft einen ersten Überblick:

- So sind Namen und Kontaktdaten der Verantwortlichen zu nennen sowie ggf. zusätzlich solche des Datenschutzbeauftragten.
- Es folgen Informationen zum Zweck der Verarbeitung und der Rechtsgrundlage der Verarbeitung.
- Werden die Daten (auch zwischen den Nutzern einer App) übermittelt, so müssen die Empfänger oder zumindest Kategorien solcher Empfänger angegeben werden. Weitere zusätzliche Angaben sind bei der Übermittlung in Drittländer gefordert.
- Eine weitere Information zur Gewährleistung einer fairen und transparenten Verarbeitung, die eine solche Erklärung beinhalten muss, sind die Dauer der Speicherung bzw. Kriterien zu deren Bestimmung.
- Wichtig ist auch, dass eine solche Erklärung Informationen über die Rechte des Betroffenen enthält. Dies umfasst das Recht auf Auskunft, das Recht auf Berichtigung und Löschung sowie die Rechte auf Einschränkung der Verarbeitung, das Widerspruchsrecht gegen bestimmte Verarbeitungen sowie auch das Recht auf Datenübertragbarkeit und das Beschwerderecht gegenüber der Aufsichtsbehörde.

- Die Angaben zum Zweck sind zu konkretisieren: So ist anzugeben, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist.
- Die Konsequenzen der Nichtbereitstellung der geforderten Daten sind zu beschreiben (bspw. Unmöglichkeit der Inanspruchnahme der Dienstleitung).
- Sollte es zu einer automatisierten Entscheidungsfindung, insbesondere zum Profiling, kommen, so verlangt die DSGVO „aussagekräftige" Informationen zur dahinterstehenden Logik und zur Tragweite und Bedeutung der so getroffenen Entscheidung für den Betroffenen. Im Vergleich zu den bisherigen Regelungen in § 34 Abs. 2 u. Abs. 4 BDSG („Wahrscheinlichkeitswerte") fällt die Formulierung deutlich unpräziser aus. Bisher wurde basierend darauf eine Offenlegungspflicht für die Scoringformel selbst verneint. Dies bleibt auch zukünftig der Fall.
- Schlussendlich werden alle oben genannten Angaben erneut für Konstellationen verlangt, für die sich die Verantwortliche Stelle die Verarbeitung zu einem weiteren Zweck vorbehalten möchte.

Die Informationspflichten entfallen, wenn der Betroffene über die Informationen bereits verfügt.

Eine tabellarische Darstellung der notwendigen Informationen mit Erläuterungen enthält Artikel 29-Gruppe, Working Paper WP260 Guidelines on transparency under Regulation 2016/679, S. 31 ff. http://t1p.de/us0z [Artikel 29-Gruppe, kostenfrei].

cc) Sonderfall: Kennzeichnungen

Eine Regelung zur Kennzeichnung einer Datenverarbeitung besteht für die Videoüberwachung von öffentlich zugänglichen Räumen (§ 4 Abs. 2 BDSG). Sie führt die bisherige Regelung zur Videoüberwachung weiter. Da die DSGVO insgesamt keine technikspezifischen Vorgaben enthält, fehlt auch eine solche für die Videoüberwachung. Eine Kennzeichnung entspricht aber den Grundprinzipien der Transparenz und der Erkennbarkeit der Datenverarbeitung.

Nötig sind geeignete Maßnahmen, um die Betroffenen auf die Überwachung aufmerksam zu machen. Gängig sind hierfür Hinweisschilder, die neben dem Umstand der Beobachtung zusätzlich Angaben zur Identität der Verantwortlichen Stelle enthalten müssen, sofern dies durch die Gesamtumstände nicht ohnehin klar erkennbar ist.

Sinnvoll kann die Kennzeichnung nur dann sein, wenn die Schilder so platziert werden, dass der Betroffene vor Betreten des Aufnahmebereiches („frühestmöglicher Zeitpunkt", § 4 Abs. 2 BDSG) auf die Beobachtung hingewiesen wird.

Die Kennzeichnung stellt schon jetzt einen der Bereiche dar, in denen sich Piktogramme durchgesetzt haben. Die Verwendung eines Videokamerasymbols ist hier gängig und erfüllt die Kennzeichnungspflicht.

c) Benachrichtigung

Informationspflichten können ihre Wirkung nur in Fällen entfalten, in denen Daten direkt bei und von dem Betroffenen selber erhoben werden. Man spricht hier von der sog. Direkterhebung. Erfolgt die Erhebung jedoch an anderer Stelle, so treten Benachrichtigungspflichten an die Stelle der Unterrichtungspflichten. Sie dienen auch als Vorstufe zu einer späteren Auskunft: Ohne Wissen von der Erhebung wird ein Auskunftsverlangen der Verantwortlichen Stelle gegenüber kaum entstehen.

aa) Verfahren und Form

Über Art. 13 DSGVO hinausgehend enthält Art. 14 DSGVO genauere Pflichten zum Zeitpunkt der Benachrichtigung, da diese eben nicht als Unterrichtung direkt bei Erhebung stattfindet. So ist innerhalb einer angemessenen Frist nach Erhebung der personenbezogenen Daten der Betroffene hierüber in Kenntnis zu setzen, spätestens jedoch nach einem Monat. Gerade bei großen Mengen von Daten wird die Verantwortliche Stelle hier schon im Vorfeld Verfahren vorgesehen haben müssen, um diesem Erfordernis nachzukommen.

Werden die Daten zur Kommunikation mit dem Betroffenen genutzt, so sind die Informationen spätestens mit dieser Kontaktaufnahme bereitzustellen. Die Monatsfrist gilt dann nicht.

Dasselbe gilt, wenn die Offenlegung der Daten an einen Dritten beabsichtigt ist. Spätestens im Zeitpunkt dieser Übermittlung muss die Information darüber erfolgen. Zu klären ist auch im Verhältnis mehrerer Verarbeiter, wer im Zweifel der Informationspflicht nachkommt. Die Informationspflichten bestehen grundsätzlich nebeneinander, sofern der Betroffene nicht bereits über die Information verfügt (s. Art. 13 Abs. 4, Art. 14 Abs. 5 lit. a DSGVO). Hier ist eine Absprache der Beteiligten bei Übermittlungen notwendig. Doppelte Informierung ist insoweit freilich nicht schädlich, ein Verlassen auf den jeweils anderen ohne Absprache aber riskant.

Auch besteht keine Pflicht, wenn die Informierung unmöglich ist oder einen unverhältnismäßigen Aufwand erfordert. Letzteres wird in der nachfolgenden Aufzählung konkretisiert: Insbesondere kommt die Unverhältnismäßigkeit bei im öffentlichen Interesse liegenden Verarbeitungen wie zu Archivzwecken, wissenschaftlichen oder historischen Forschungszwecken oder für statistische Zwecke in Frage. Die Bedeutung der Ausnahme dürfte sich außerhalb dieser Fälle daher wohl in engen Grenzen halten.

Ausnahmen können sich ergeben, wenn die Erlangung oder Offenlegung der Daten durch ein anderes Gesetz vorgesehen ist oder die Daten einer Geheimhaltungspflicht oder einem Berufsgeheimnis unterliegen. In diesen Fällen können sich aber Benachrichtigungspflichten auch aus dem jeweiligen Spezialgesetz ergeben.

Im Gegensatz zu den geschilderten Unterschieden im Verfahren, gibt es für die Form keine weiteren Unterschiede zu Art. 12 DSGVO. Insoweit kann somit auf obige Ausführungen verwiesen werden (III.1.b.aa.).

bb) Inhaltliche Anforderungen

Die inhaltlichen Anforderungen ergeben sich ebenfalls aus Art. 14 DSGVO. Diese entsprechen in weiten Teilen den bereits oben beschriebenen Informationen aus Art. 13 DSGVO, wenn auch die Gliederung innerhalb der Norm vereinzelt abweicht. Daneben gelten die allgemeinen Grundsätze zu Transparenz und Verständlichkeit aus Art. 12 DSGVO.

Auch hier sind nicht die personenbezogenen Daten selbst Gegenstand der Benachrichtigung.

Als über Art. 13 DSGVO hinausgehende zusätzliche Information ist bei der Benachrichtigung zusätzlich die Quelle, aus der die Daten stammen anzugeben sowie gegebenenfalls, ob es sich dabei um eine öffentlich zugängliche Quelle handelt.

d) Auskunft

Unabhängig von der Unterrichtung und Benachrichtigung hat der Betroffene stets ein Recht auf Auskunft. Dieses Recht unterscheidet sich in zwei wesentlichen Aspekten von den vorherigen Pflichten:

- Einerseits geht es hier nicht mehr abstrakt um die Art der erfassten Daten, sondern um die konkret gespeicherten Informationen. Dies ermöglicht dem Betroffenen auch erstmals eine inhaltliche Nachprüfung.

- Andererseits besteht hier keine Pflicht für die Verantwortliche Stelle, proaktiv tätig zu werden, sondern lediglich ein Anspruch des Betroffenen, auf den dann reagiert werden muss.

Nichtdestotrotz ist im Falle eines Auskunftsverlangens eines Betroffenen natürlich auch hier aus Sicht der Verantwortlichen Stelle auf eine rechtssichere und auch ansonsten positive und konstruktive Kommunikation zu achten.

aa) Verfahren und Form

Die zentrale Regelung zum Auskunftsrecht ist Art. 15 Abs. 3 DSGVO.

Anders als der frühere § 34 Abs. 8 BDSG, welcher den Anspruch grundsätzlich auf eine Auskunft einmal im Jahr beschränkte, ist in der DSGVO kein festgeschriebenes Intervall mehr vorgesehen, was eine gewisse Unsicherheit schafft. ErwGr. 63 spricht aber jedenfalls von „angemessenen Abständen". Die Auskunft bleibt weiterhin grundsätzlich kostenlos, wobei Art. 15 Abs. 3 S. 2 DSGVO für weitere Kopien ein Entgelt zulässt. Eine Orientierung an der jährlichen Auskunft des früheren BDSG scheint in vielen Fällen wohl sinnvoll. Bei sich häufig verändernden Daten wäre ohne eine solche Festlegung aber auch eine häufigere Auskunft denkbar. Eine Grenze setzt hier Art. 12 Abs. 5 DSGVO zur Verhinderung vielfacher, exzessiver oder offensichtlich unbegründeter Anträge. Den Nachweis dafür muss die Verantwortliche Stelle erbringen. Zur Höhe des Entgelts erwähnt Art. 15 Abs. 3 DSGVO als Grundlage die tatsächlich entstandenen Verwaltungskosten. Keine Stellungnahme ist zu eventuellen Hinweispflichten vor Erhebung eines Entgelts zu finden.

Von den Auskunftspflichten und dem neugeschaffenen Zugangsrecht enthält Art. 15 Abs. 4 DSGVO eine im Vergleich zum bisherigen deutschen Recht sehr knappe Ausnahmeregelung. So darf ein Datenauszug gem. Art. 15 Abs. 4 DSGVO lediglich die Rechte und Pflichten anderer Personen nicht beeinträchtigen. Zur Erläuterung zählt ErwGr. 63 beispielhaft Geschäftsgeheimnisse und Rechte des geistigen Eigentums, insbesondere Urheberrechte an Software, auf. Dies solle allerdings nicht zu einer völligen Verweigerung der Auskunft führen.

Ähnliche Ausführungen wie in Art. 14 DSGVO bei Unmöglichkeit, Unverhältnismäßigkeit oder bei Bestehen von Berufsgeheimnissen fehlen. Diese lassen sich aber problemlos in die weite Formulierung des Art. 15 Abs. 4 DSGVO hineinlesen.

Außerdem ist die für die Bearbeitung solcher Anträge nötige Infrastruktur zu schaffen.

Formvorgaben oder Begründungspflichten für den Antrag gibt es nicht. ErwGr. 63 der DSGVO sieht aber wie auch das bisherige Recht grundsätzlich vor, dass der Betroffene die Daten, zu denen er Auskunft begehrt, insbesondere gegenüber Unternehmen und Behörden, die große Mengen von Daten verarbeiten, präzisieren muss, damit diese auffindbar sind. Aus praktischer Sicht scheint ein anderes Vorgehen kaum denkbar.

bb) Inhaltliche Anforderungen

Es ist dem Betroffenen auf Antrag eine „Kopie" aller verarbeiteten Daten zu überlassen. Bisher war davon auszugehen, dass der Betroffene so informiert werden muss, dass er auch ohne Vorkenntnisse, Hilfsmittel oder gar fachliche Beratung feststellen kann, welche Daten über ihn gespeichert worden sind.

2. Proaktive Kommunikation mit Datenschutzaufsichtsbehörden

***v. Lewinski**, Formelles und informelles Handeln der datenschutzrechtlichen Aufsichtsbehörden, RDV [Recht der Datenverarbeitung] 2001, S. 275 ff.*

Schon an dieser Stelle soll kurz die Bedeutung der Kommunikation mit den Datenschutzaufsichtsbehörden erwähnt werden. Auch wenn Aufsicht aus Sicht der Verantwortlichen Stelle häufig eher im Zusammenhang mit Verstößen und Sanktionen eine Rolle spielt, sollte die Ebene des informellen Austausches und der faktischen Zusammenarbeit mit diesen für den Datenschutz nicht unterschätzt werden. In den obigen Absätzen, beispielsweise bezüglich der Datenschutz-Folgenabschätzung, wurden diesbezüglich schon einige kooperative Elemente der DSGVO angesprochen.

a) Kein vorgeschriebenes Verfahren

Auch unter der DSGVO gehört die Beratung der Verantwortlichen Stelle durch die Aufsichtsbehörden zu deren Aufgabenbereich (Art. 57 Abs. 1 lit. d, lit. l DSGVO). Diese wird bereits als Kontroll- und Einwirkungsinstrument der Aufsichtsbehörden angesehen. Die Beratung wirkt dabei häufig in beide Richtungen: die Verantwortliche Stelle kann sich auf diesem Wege informieren, und auch die Aufsichtsbehörde bringt so branchenübliches Verhalten und Besonderheiten in Erfahrung, die ihr weiteres Tätigwerden beeinflussen können. Durch die generalklauselartige Ausgestaltung des neuen Datenschutzrechtes, viele unbestimmte Rechtsbegriffe und dem bewussten Verzicht der DSGVO auf technikspezifische Regelungen, ist die Bedeutung der informellen Zusammenarbeit trotz einer graduellen Verschärfung der Aufsicht und der Bußgelder auch für die Zukunft weiterhin als hoch einzuschätzen.

b) Inhalt

Bezüglich des Kommunikationsinhaltes sind aus rechtlicher Sicht kaum Grenzen zu ziehen. Rein praktisch wird die Aufsichtsbehörde aber natürlich keine Beratung über ihren Aufgabenbereich hinaus leisten können, wollen und dürfen.

Auch kann sich eine zu offene Kommunikation aus Sicht der Verantwortlichen Stelle möglicherweise im Einzelfall negativ auswirken. So ist eine direkte Information über bußgeldwerte oder gar strafbare Verstöße („Selbstbezichtigung“) innerhalb eines informellen Verfahrens ohne fundierte juristische Beratung kaum zu empfehlen. Ebenso ist eine pauschale und eigenmächtige Öffnung interner Informationen für die Datenschutzaufsicht nicht ratsam. Anders als in anderen Rechtskreisen kennt das deutsche Recht zudem keine pauschalen Verwertungsverbote. Dies gilt insbesondere für sog. „Zufallsfunde“, die ein freier Zugang über die eigentlich zu klärenden Vorgänge hinaus ermöglichen könnte. Hier drohen erhebliche Konsequenzen.

c) Verwendung in der Datenschutzkommunikation

Ein gutes Verhältnis und eine offene Kommunikation mit den Aufsichtsbehörden können hier also schon im Vorfeld mögliche Verarbeitungsrisiken aufdecken und Haftungsrisiken langfristig reduzieren.

3. Kombination von rechtlicher Eindeutigkeit und Betroffenenverständlichkeit

Unabhängig davon, ob nun für eine Einwilligung informiert wird, bei einer Direkterhebung unterrichtet, anschließend benachrichtigt oder Auskunft gegeben wird, immer geht es darum, die rechtlichen Anforderungen mit einer adressatengerechten Formulierung zu kombinieren.

a) Rechtliche Vorgaben

Die allgemeinen Leitlinien zur Information und Kommunikation mit dem Betroffenen gibt Art. 12 DSGVO vor.

Informationen sind transparent, leicht zugänglich und verständlich zu gestalten. Dabei ist eine klare und einfache Sprache zu verwenden. Es scheint diesbezüglich sinnvoll, sich im Ausgangspunkt bei dieser Beurteilung am durchschnittlichen Betroffenen zu orientieren. Gerade bei Internetangeboten mit multinationaler Zielgruppe wird man auch davon ausgehen müssen, dass die erhöhten Anforderungen an die Verständlichkeit nur durch eine Bereitstellung von Informationen in unterschiedlichen Sprachen erfüllt werden können. Besonders betont werden diese Anforderungen noch einmal, wenn sich das Angebot an Kinder richtet. Eine kindgerechte und gleichzeitig rechtlich und technisch fundierte Kommunikation dürfte hier eine besondere Herausforderung darstellen.

Umstritten scheint hier bisher noch zu sein, inwieweit dafür auch (programm)technische Vorgänge der Datenverarbeitung dem Betroffenen gegenüber in allen Einzelheiten offengelegt werden müssen (so z.B. Art. 13 Abs. 2 lit. f DSGVO u. Art. 14 Abs. 2 lit. g DSGVO) zu automatisierten Einzelentscheidungen). Eine zu technische Beschreibung kann dem Ziel einer transparenten Kommunikation jedenfalls kaum gerecht werden.

Auch zur Form der Mitteilung nimmt Art. 12 DSGVO Stellung. So kann die Mitteilung schriftlich, in anderer Form oder auch elektronisch, in Ausnahmefällen bei Zustimmung des Betroffenen sogar mündlich erfolgen. Hierbei ist aber zu beachten, dass der Betroffene seine Identität auf anderem Wege nachgewiesen haben muss. Verstanden wird diese Regelung als Eröffnung einer weitestgehenden Formfreiheit in diesem Bereich. Nach ErwGr. 58 soll bei öffentlich zugänglichen Informationen die Bereitstellung auf einer Website (s. dazu III.1.b.) genügen. Dies entspricht letztendlich dem bereits heute üblichen Vorgehen bei Datenschutzerklärungen.

b) Sanktionen

Die Nichteinhaltung der rechtlichen Vorgaben zur Kommunikation ist unter der DSGVO sanktionierbar. Es drohen für bestimmte Verstöße Bußgelder von bis zu 10 Millionen Euro oder bei Unternehmen bis 2% des weltweiten Jahresumsatzes (Art. 83 Abs. 4 DSGVO) oder für andere sogar bis zu 20 Millionen Euro oder 4% des Jahresumsatzes (Art. 83 Abs. 5 DSGVO). Nach Art. 83 Abs. 7 DSGVO sind ähnliche Regelungen nach nationalem Recht grundsätzlich auch für Behörden und öffentliche Stellen denkbar.

Die Missachtung der allgemeinen Vorgaben für die Kommunikation aus Art. 12 DSGVO, sowie die spezielleren Vorgaben zur Information, Benachrichtigung und zu den einzelnen Rechten der Betroffenen, fallen in die letztere, teurere Kategorie.

Die Nichterstellung eines Verfahrensverzeichnisses fällt unter die Bußgeldandrohung des Art. 83 Abs. 4 DSGVO. Schon unter Geltung des BDSG ergaben Umfragen, dass einige Unternehmen ein solches Verzeichnis überhaupt nicht führten. Das Bußgeld sollte diesbezüglich, neben den aufgezeigten weiteren Verwendungen in der Kommunikation, ein zusätzlicher Anreiz sein.

Die Einhaltung der Pflichten und insgesamt die Zusammenarbeit mit den Aufsichtsbehörden sind dabei Faktoren für die spätere Bußgeldbemessung. Schon anfänglich gelebte Transparenz und gute Kommunikationsstandards zahlen sich hier also im Falle einer Datenpanne durch ihre positive Berücksichtigung langfristig aus. Insbesondere ein Code of Conduct oder eine Zertifizierung ist hier geeignet das Bußgeld zu reduzieren. Ein frühes Bekenntnis zum Datenschutz kann der Verantwortlichen Stelle hier also zum Vorteil gereichen.

c) Darstellungsvarianten für die Betroffenen-Information

***Nationaler IT Gipfel** 2015, Datenschutzhinweise („One Pager"), verfügbar unter: http://t1p.de/vph5 [BMJV, kostenfrei]; Erläuterungen dazu: http://t1p.de/r98m [BMJV, kostenfrei] // **Artikel 29-Gruppe**, Working Paper (WP) 260 Guidelines on transparency under Regulation 2016/679, http://t1p.de/us0z [Artikel 29-Gruppe, kostenfrei] // **Ermakova/Baumann/Fabian/Krasnova**, Privacy Policies and Users' Trust: Does Readability Matter?, AMCIS 2014; Sultan/Urban/Shankar/Bart, Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers?, 2002, abrufbar unter: http://t1p.de/bu7h [SSRN, kostenfrei] // **Ermakova/Fabian/Babina**, Readability of Privacy Policies of Healthcare Websites, S. 2, abrufbar unter https://researchgate.net/publication/268981590 [ResearchGate, kostenfrei]*

Schon im Bereich des (bisherigen) § 13 TMG gab es umfangreiche Bestrebungen, eine gegenüber den Betroffenen möglichst verständliche und transparente Kommunikation sicherzustellen. Die Artikel 29-Gruppe betont in ihrem oben angeführten Working-Paper insbesondere sog. „layered privacy-statements". Nur bestimmte Abschnitte und Zusammenfassungen bieten einen ersten Überblick und ein Klick auf die jeweiligen Bereiche ermöglicht dem Betroffenen eine weitere, detaillierte Information.

Als gelungenes Beispiel zur Orientierung kann hier der vom Nationalen IT-Gipfel 2015 erarbeitete einseitige Datenschutzhinweis nebst Erläuterungen für den Verarbeiter angeführt werden. Zwar ersetzt auch dieses Dokument nicht vollständig die noch zusätzlich zu erstellende Datenschutzerklärung selbst, es fasst diese aber übersichtlich und allgemeinverständlich zusammen. Insbesondere begrüßenswert bei diesem Ansatz ist der Abschnitt, der den Betroffenen über seine Rechte bezüglich Auskunft, Löschung, Berechtigung und Widerspruch informiert, der nunmehr um die Rechte auf Datenübertragung sowie des Rechts auf Einschränkung der Verarbeitung ergänzt werden müsste. Das Fehlen der Informationen über Betroffenenrechte stellte laut der Stiftung Warentest einen der am häufigsten festzustellenden Mängel dar (test 3/2016, S. 59–61), was im Hinblick auf die oben angesprochenen Verpflichtungen hierzu aus Art. 13 Abs. 2 lit. b und Art. 14 Abs. 2 lit. c DSGVO zwingend zu ändern ist.

Zu denken ist dabei auch an die Vermittlung von Informationen in Audioformaten für Menschen mit Sehbeeinträchtigung. Je nach Art der Kommunikation sind für den speziellen Einsatzzweck auch neue Mittel der Information zu erwägen, da insbesondere bei „Internet of Things"-Anwendungen die Information durch einen Text häufig kaum umsetzbar erscheint (dazu die weiterhin geltende Artikel 29-Gruppe, Opinion 8/2014, http://t1p.de/6izs, kostenfrei).

Als angemessen kann sich dabei je nach Situation die Information auf Papier, der Telefon, durch QR-Codes, Audionachrichten, mündliche Erklärungen oder öffentlich sichtbare Kennzeichnung erweisen (s. für umfangreiche Praxisbeispiele Artikel 29-Gruppe, Working Paper (WP) 260, Guidelines on transparency under Regulation 2016/679, S. 18 f. http://t1p.de/mvet kostenfrei). Der einfache Zugang zu Informationen kann auch durch Popup-Fenster, Auflistung der wichtigsten Informationen im Rahmen von FAQ-Übersichten oder sogar durch den Einsatz interaktiver digitaler Dienste wie z.B. Chatbots sichergestellt werden. Zudem sind (Kurz-)Videos denkbar, in denen der Verantwortliche die Gründe für eine (notwendige) Datenerhebung erklärt.

Ein weiterer interessanter Kommunikationsansatz ist der sog. „Nutrition Label Approach", der sich an den bekannten und im Grundsatz bewährten tabellarischen Angaben auf Nahrungsmitteln und ähnlichen Kennzeichnungen wie z.B. bei der Energieeffizienz von Elektrogeräten orientiert. Im Rahmen einer Untersuchung zur Wirksamkeit solcher Labels wurde auch eine grobe Klassifizierung der Gestaltungsformen solcher Erklärungen vorgenommen: Man kann zwischen einer tabellarischen Darstellung, einer verkürzten tabellarischen Darstellung, einem Kurz-Text, einem vollständigen Fließtext sowie einer in tabellarische Blöcke aufgeteilten Textdarstellung unterscheiden. Der oben angeführte „One Pager" des IT-Gipfels ließe sich hier in die Kategorie der in tabellarische Blöcke aufgeteilten Textdarstellung einordnen.

Beispiel für eine tabellarische Darstellung:

Unternehmensname
Name des Verantwortlichen
Anschrift
Tel./Fax/Email

betriebl. Datenschutzbeauftragte
Kontaktdaten

Wir verwenden die Daten... / Erfasste Daten	...zur Nutzung unserer Dienste und der Website	...für Werbezwecke	...für Telemarketing	...für Profiling	...zur Weitergabe an andere Unternehmen	...zur Weitergabe an öffentliche Stellen
Folgen der Nichtbereitstellung	**Keine Nutzung möglich**	**Keine aktuellen Angebote**		**Keine Nutzung möglich**	**keine Partner-Angebote**	
Kontaktdaten		Opt-in			Opt-out	
Cookies						
Demographische Daten		Opt-in			Opt-out	
Finanzdaten						
Gesundheitsdaten						
Präferenzen						
Kaufinformationen		Opt-in			Opt-out	
Ausweisnummer						
Aktivitäten auf unserer Web-Seite		Opt-in			Opt-out	
Ihr Standort						

In Zusammenhang mit der Datenverarbeitung stehen Ihnen umfangreiche gesetzliche Rechte zu:

Recht auf Widerruf der Einwilligung	**Anspruch auf Berichtigung**	**Anspruch auf Löschung**	**Anspruch auf Einschränkung der Verarbeitung**	**Recht auf Widerspruch**
	Auskunft über gespeicherte Daten	**Beschwerderecht bei der Aufsichtsbehörde**	**Recht auf Datenübertragbarkeit**	

Legende:
grün: Sie entscheiden, ob wir Ihre Daten erfassen.
gelb: Auf Ihren Wunsch hin verzichten wir auf die Datenerfassung.
rot: Ohne die Erfassung dieser Daten kann unser Service leider nicht genutzt werden.

***Nach P.G. Kelley, L.J. Cesca, J. Bresee, and L.F. Cranor**, Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach. CHI 2010.*

Alle beschriebenen Ansätze können im Hinblick auf die detaillierten Vorgaben der DSGVO nur als erste Übersicht und somit gewissermaßen als zusätzliches Angebot für den Betroffenen im Rahmen einer gelungenen Kommunikationsstrategie gesehen werden. Diesen muss jedoch aus rechtlichen Gründen weiterhin eine um-

fangreiche Datenschutzerklärung folgen. Daneben bedürfen gerade die tabellarischen Darstellungen zu ihrer Verständlichkeit noch ergänzend beigelegten Erläuterungen. Dabei ist auf die Widerspruchsfreiheit zwischen den bloßen Datenschutzhinweis, und der eigentlichen Datenschutzerklärung zu achten.

Gerade durch diese nach der Informationsdichte gestaffelte Kommunikation können sich Unternehmen deutlich von ihrer Konkurrenz abheben und somit Wettbewerbsvorteile im Bereich der Datenschutzkommunikation schaffen. Die Lesbarkeit und Verständlichkeit der Datenschutzerklärung erhöhen nicht nur das Vertrauen der Nutzer in die Erklärung selber, sondern auch in die Datenschutzstrategie des dahinterstehenden Unternehmens.

d) Ergänzender Einsatz von Piktogrammen

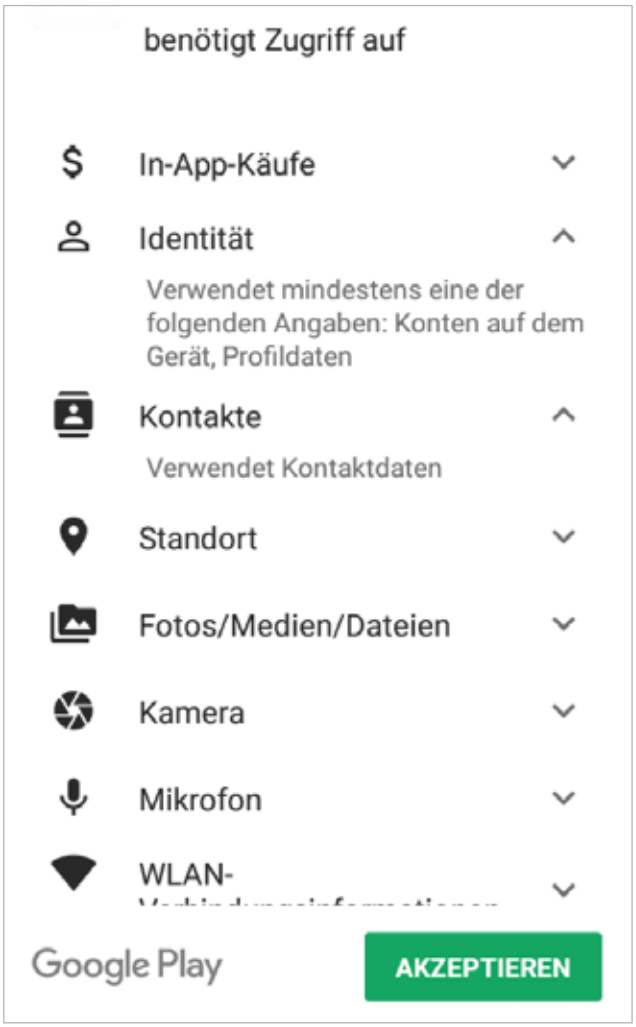
***Richter**, Simplifizierung als Lösung für die „Daten-AGB? “, PinG [Privacy in Germany] 2017, 65 abrufbar unter http://t1p.de/c9ca [PinG, kostenpflichtig]*

Alle Ansätze ließen sich mit denen von der DSGVO angedachten Piktogrammen verbinden (Art. 12 Abs. 7 DSGVO). Bis zur Erstellung dieser durch den Europäischen Datenschutzausschuss (Art. 12 Abs. 8 DSGVO) bleibt aber abzuwarten, ob diese in ihrer tatsächlichen Form geeignet sind, die gesetzlich notwendigen komplexen Informationen für den durchschnittlichen Anwender verständlich darzustellen. Ansätze in diese Richtung gab es bereits einige. Zu nennen seien einerseits das p3p-Projekt, was auf Protokollebene eine Vereinheitlichung der angezeigten Datenschutzinformationen erreichen wollte, und diverse daran anknüpfende Projekte wie beispielsweise „Mozilla Privacy Icons“ oder „KnowPrivacy“. Leider ist den Projekten gemeinsam, dass sie nie große Praxisrelevanz erreichen konnten und eine Weiterentwicklung daher eingestellt wurde. Wenig überzeugend war in diesem Zusammenhang auch der Vorschlag des EU-Parlaments [abrufbar unter http://t1p.de/qqk5; EU- Parlament, kostenfrei, S. 333].

Zur Veranschaulichung hier einige Beispiele, die optisch an die Creative-Commons Lizenzsymbole erinnern:

aus „Iconset for Data-Privacy Declarations v 0.1“ von Matthias Mehldau (bearbeitet)
Lizenz: Creative Commons Namensnennung 2.0 Deutschland, http://creativecommons.org/licenses/by/2.0/de/

Ein gelungenes Beispiel der Kombination von Datenschutz-Informationen und Piktogrammen findet sich in der Android App „Google Play Store“. Zwar handelt es sich bei den dort hinterlegten Angaben strenggenommen um Angaben zur betriebssystemseitigen Rechtevergabe für das Programm, jedoch beziehen sich viele der Angaben auch auf die beabsichtigte Datenverarbeitung und -weitergabe:



Aus der Android App „Google Play Store", Vers. 7.6.08.N-all [0] [PR] 149245622 auf Android 5.0 build 2.0.1_20150623-1900

e) Ausgestaltungsmöglichkeiten für das Auskunftsverfahren

In Erwägungsgrund 63 der DSGVO enthält das europäische Recht eine echte kommunikative Neuheit, indem es als zulässig erklärt wird, dass Betroffenen ersatzweise statt der reaktiven Auskunft im Einzelfall ein elektronischer Zugang zu seinen Daten ermöglicht wird. Dies gibt dem Auskunftsrecht eine neue, weitreichende Bedeutung. Denkbar wäre dadurch einerseits für den Betroffenen eine Echtzeitkontrolle der Datenbestände und somit größere Transparenz. Andererseits könnte bei ohnehin auf Webservern vorhandenen Daten der Aufwand für die Verantwortliche Stelle durch diese Möglichkeit der Selbstauskunft auf Dauer deutlich reduziert werden: Der Betroffene gibt bzw. nimmt sich selber Auskunft.

Ähnlichkeiten lassen sich hier zum Konzept des sog. „Datenbriefes" – das wohl auf Arthur R. Miller, The Atlantic, Ausgabe 220, Nr. 5 (1967), S. 53 (55 f.), zurückgeht und in Deutschland von Simitis (NJW 1971, S. 673, 681 f.) aufgegriffen und eine Zeit lang vom Chaos Computer Club (CCC) propagiert worden war – als einer Art „Datenkontoauszug" erkennen. Zwar ist eine solche (einmalige oder periodische) zusammenfassende Mitteilung über die gespeicherten Daten bisher nicht gesetzlich vorgesehen, der Erwägungsgrund 63 eröffnet aber Möglichkeiten, über diese Idee noch weit hinauszugehen. Schon beim Modell des Datenbriefes war von einem Kommunikationsstandpunkt an die Möglichkeit von Beilagenwerbung zu denken. Dauerhaft zugängliche, digitale Auskunftssysteme könnten auch hier Synergie-Effekte bringen, indem der Kunde hierdurch bereits auf die unternehmenseigene Website gelotst wird.

Einige Anbieter haben sich zu einem recht umfangreichen Angebot entschlossen. Als bekannte Beispiele seien hier exemplarisch die Facebook-Funktion „Eine Kopie deiner Facebook-Daten herunterladen“, die neben der Auskunft auch den Download erlaubt, und die Unterseite „Meine Aktivitäten“ in den Konten-Einstellungen bei Google genannt.

IV. Reaktive Kommunikation

***Belke/Neumann/Zier**, Datenschutzalltag in deutschen Unternehmen, DuD (Datenschutz und Datensicherheit) 11/2015, S. 753 ff., abrufbar unter http://t1p.de/y1cz [Springer Link, kostenpflichtig]*

Auch nach Ende der verarbeitungsbezogenen Datenschutzkommunikation ist die Datenschutzkommunikation noch nicht zu Ende: Meldung von Datenpannen und andere Datenschutz-Krisen-PR sind nicht nur rechtlich, sondern ebenfalls kommunikativ besonders herausfordernd.

Typische Ursache für Datenpannen und Datenschutzverstöße ist, neben dem Fehlverhalten von Mitarbeitern, die fehlende Umsetzung gesetzlicher Vorgaben bezüglich organisatorischer und technischer Maßnahmen. Auch der sorglose Umgang mit IT-Technologie oder das unbedachte Einspielen von Updates kann zu Problemen führen. Daneben ist – je nach Branche – mit vorsätzlichen Angriffen auf die Dateninfrastruktur zu rechnen.

1. Informierung bei Datenpannen: Data Breach Notifications

***Artikel 29-Gruppe**, Working Paper WP250rev.01 Guidelines on Personal data breach notification under Regulation 2016/679, http://t1p.de/k4d [Artikel 29-Gruppe, kostenfrei]*

Natürlich sollte der Fokus in der täglichen Arbeit in den vorher geschilderten Phasen liegen und Probleme mit Datenpannen durch technische und organisatorische Maßnahmen möglichst verhindert werden. Für den Fall, dass eine Datenpanne dennoch eintritt, sollte man aber vorbereitet sein. Eine Datenpanne sollte im Idealfall schnell entdeckt und anschließend beschränkt und beseitigt werden. Hierfür sind bereits im Vorfeld alle angemessenen technischen und organisatorischen Maßnahmen zu treffen.

In Fall einer Datenpanne sind aus Sicht der Datenschutzkommunikation zwei Problemkomplexe zu unterscheiden. Zum einen bestehen möglicherweise rechtliche Mitteilungspflichten. Dies kann sowohl gegenüber den Aufsichtsbehörden als auch gegenüber den Betroffenen der Fall sein. Bei vorsätzlichen Angriffen kann das Einschalten der Strafverfolgungsbehörden angezeigt sein.

a) Verpflichtung und Verfahren

In Rahmen dieser Mitteilungen muss sich die Kommunikation zwingend nah an den gesetzlichen Vorgaben orientieren, damit den dort festgelegten Pflichten nachgekommen wird. Der Spielraum ist hier eher gering. In der DSGVO ergeben sich Mitteilungspflichten aus Art. 33 und 34. Weitere Pflichten bestehen momentan noch im Rahmen der § 15a TMG; § 73 Abs. 1 S. 3 Messstellenbetriebsgesetz [MsbG]; VO (EU) 611/2013; § 109a TKG.

aa) Pflichten gegenüber der Aufsichtsbehörde

Die Aufsichtsbehörden sind nach Art. 33 Abs. 1 DSGVO über eine Verletzung des Schutzes personenbezogener Daten, unverzüglich, in aller Regel binnen 72 Stunden nach Kenntnis, zu informieren. Eine spätere Meldung muss eine Begründung für die Verzögerung beigelegt werden. Zumindest die vorhandenen Informationen sollten der Aufsichtsbehörde bereits innerhalb der Frist übermittelt und auf die noch nicht vorhandenen,

nachzureichenden Angaben hingewiesen werden. Gerade im Hinblick darauf, dass Einbrüche in die IT von Unternehmen und Behörden in Deutschland im Schnitt erst nach etwa eineinhalb Jahren entdeckt werden, ist das Abstellen auf den Moment des Bekanntwerdens essentiell. Dies kann durch ein eigenes Erkennen der Datenpanne, eine Information eines Betroffenen oder bspw. auch durch eine Medienberichterstattung eintreten.

Die Pflicht greift unabhängig von Vorsatz, Fahrlässigkeit oder Fehler Dritter. Meldepflichtig ist jede Verletzung der Sicherheit, die zu Vernichtung, Verlust, Veränderung, zu unbefugter Offenlegung oder zu unbefugtem Zugang zu persönlichen Daten führt (Art. 4 Nr. 12 DSGVO).

Die Artikel 29-Gruppe bildet in ihrem Working-Paper hierzu drei Fallgruppen:

- Die Verletzung der Vertraulichkeit der Daten: bspw. durch unberechtigten oder unbeabsichtigten Zugang zu personenbezogenen Daten
- Die Verletzung der Integrität der Daten: bspw. durch unberechtigte oder unbeabsichtigte Möglichkeit zur Änderung der Daten
- Verletzungen der Verfügbarkeit der Daten: bspw. durch unberechtigten oder unbeabsichtigten Verlust des Zugangs zu Daten

Gerade die letzte Fallgruppe sollte hier in der Praxis im Auge behalten werden, da hier der Trugschluss entstehen könne, dass ein Verlust des Zugriffs für die Verantwortliche Stelle kein meldepflichtiger Verstoß sei. Dies ist aber nach Ansicht der Artikel 29-Gruppe der Fall. Eine bloße Verletzung der IT-Infrastruktur ist hingegen nicht meldepflichtig, wenn kein Zugriff auf personenbezogene Daten erfolgt ist.

Entfallen kann die Pflicht zur Mitteilung, wenn voraussichtlich kein Risiko für Rechte und Freiheiten von natürlichen Personen besteht (Art. 33 Abs. 1 Hs. 2 DSGVO). In Zusammenschau mit den Haftungs- und Sanktionsvorschriften ist hier vor allem auf die Wahrscheinlichkeit des Eintritts von materiellen und immateriellen Schäden abzustellen (vgl. Erwägungsgrund 85 der DSGVO). Je nach Art der gespeicherten Daten und Umfang eines Datenverlusts bestehen hier ganz erhebliche Risiken, es sei denn, die Daten wurden allein im Interesse des Verantwortlichen erhoben, unterliegen nicht besonderen gesetzlichen oder vertraglichen Aufbewahrungspflichten und es ist ausgeschlossen, dass Dritte die Daten zur Kenntnis genommen haben („Laptop fällt auf hoher See ins Wasser"; Verschlüsselung nach dem Stand der Technik). Die Prognose ist dabei methodisch sorgfältig zu erstellen und im Nachhinein gerichtlich voll überprüfbar. Zu berücksichtigende Risiken sind die Einschränkung von Rechten, Diskriminierung, Identitätsdiebstahl, finanzielle Verluste, die unberechtigte Rückgängigmachung von Pseudonymisierung, Rufschädigungen, Verlust der Vertraulichkeit bestimmter Daten insb. auch in Verbindung mit Berufsgeheimnissen.

Empfohlen wird von den Aufsichtsbehörden daher die Erstellung einer umfassenden Dokumentation über Datenpannen, unabhängig vom Bestehen der Meldepflicht. Mithilfe dieser Dokumentation kann bei einer Überprüfung nachgewiesen werden, dass eine Informierungspflicht nicht bestand und es können die Gründe für ein Überschreiten der 72-Stunden-Frist plausibel gemacht werden.

bb) Pflichten gegenüber den Betroffenen

In besonderen Fällen sind zusätzlich die Betroffenen selber zu informieren. Die Regelungen hierzu enthält Art. 34 DSGVO. Die Meldepflicht den Betroffenen gegenüber tritt allerdings nur in dem Fall ein, dass ein „hohes Risiko" für deren Rechte und Freiheiten besteht. Während die Mitteilung an die Aufsichtsbehörde im Fall einer Verletzung also im Zweifel erfolgen sollte, ist die an den Betroffenen selbst die Ausnahme. Art. 34 Abs. 3 DSGVO enthält darüber hinaus noch konkretere Fälle, in denen die Mitteilung an die Betroffenen in jedem Fall ausscheidet. Dies gilt vor allem bei Abhandenkommen ohnehin ausreichend verschlüsselter Daten (lit.

a), bei Ausschluss eines hohen Risikos für die Betroffenen zwischen Mitteilung an die Aufsichtsbehörde und möglicher Benachrichtigung der Betroffenen (lit. b) und insbesondere in dem Fall, wenn die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre (lit. c). Im letzten Fall ist das allerdings ersatzweise eine öffentliche Bekanntmachung oder ähnlich wirksame Maßnahme zur Informierung zu treffen. Die möglichen kommunikativen Folgen einer solchen öffentlichen Mitteilung sollten bei der Entscheidung, sich auf einen unverhältnismäßigen Aufwand zu berufen, berücksichtigt werden.

Wann ein „hohes Risiko" für die Rechte und Freiheiten Betroffener vorliegt, ist wiederum von der DSGVO nicht ausdrücklich festgelegt. Der Europäische Datenschutzausschuss wird Leitlinien festlegen. Maßgeblich zu berücksichtigen sind neben physischen und psychischen Schäden auch Diskriminierungsgefahren, der Grad der Rufschädigung und mittelbare Auswirkungen auf die freie Entfaltung der Persönlichkeit im Privat- und Berufsleben des Betroffenen. Dabei muss aber gleichzeitig die Eintrittswahrscheinlichkeit des Schadens zumindest signifikant erhöht sein (vgl. zur Orientierung die Erwägungsgründe 75 u. 85).

cc) Haftung und Sanktionen

Gerade für den Fall einer Datenpanne ist auf die damit verbunden Haftungs- und Sanktionsrisiken hinzuweisen.

Dies gilt einmal in Anknüpfung an die Panne selbst: Nach Art. 82 Abs. 1 DSGVO ist eine umfangreiche Haftung für materielle oder immaterielle Schäden vorgesehen, die dem Betroffenen aus Verstößen entstehen.

Daneben sind die obigen Kommunikationspflichten aus Art. 33 und 34 DSGVO gegenüber Aufsichtsbehörde und Betroffenem bußgeldbewehrt, Art. 83 Abs. 4 DSGVO. Nicht nur aus Kommunikationssicht bestehen hier also große Anreize für eine gute Informierung.

b) Inhaltliche Anforderungen

Den Inhalt der Meldung beschreibt Art. 33 Abs. 3 DSGVO. Dies umfasst eine möglichst detaillierte Angabe der betroffenen Daten und der möglichen Anzahl von Betroffenen, die Angabe von Kontaktdaten für die Aufsichtsstelle für weitere Rücksprache, insbesondere auch die Kontaktdaten des möglicherweise benannten Datenschutzbeauftragten. Darüber hinaus sind eine Beschreibung der wahrscheinlichen Folgen der Datenpanne und der von der Verantwortlichen Stelle bereits getroffenen oder vorgeschlagenen Maßnahmen zur Eindämmung des Problems nötig.

Von der Artikel 29-Gruppe werden als Beispiele für Beschreibungen der Betroffenengruppen Kinder, andere benachteiligte Gruppen, Menschen mit Behinderung, Arbeitnehmer oder Kunden angeführt. Mögliche Arten von betroffenen Daten könnten bspw. Gesundheitsdaten, Bildungsbiographien und Noten, Daten mit sozial- und Pflegebezug, Finanzdaten, Bankdaten, Ausweisnummern oder ähnliches sein.

Gerade die Zahl der Betroffenen kann dabei auch geschätzt werden und muss innerhalb von 72 Stunden nicht präzise ermittelt werden.

Die Informationen können gemäß Art. 33 Abs. 4 DSGVO später nachgereicht werden, sofern dies im Einzelfall nicht anders möglich ist. Art. 33 Abs. 5 DSGVO verlangt darüber hinaus das Anlegen einer umfangreicheren, überprüfbaren Dokumentation der Verletzung selber und der zur Minderung der Folgen getroffenen Maßnahmen.

Die Mitteilung an den Betroffenen selbst ist in klarer und einfacher Sprache zu verfassen (Art. 34 Abs. 1 DSGVO). Diesbezüglich kann auf die obigen Ausführungen zu zielgruppenorientierter Kommunikation verwiesen

werden (II.3.b.cc.). Abweichungen von den möglicherweise sehr juristisch oder technisch geprägten Ausführungen für die fachlich vorgebildeten Aufsichtsbehörden sind hier empfehlenswert.

c) Zusätzliche Felder der Kommunikation von Datenpannen

***Bräuning/Thießen**, Reden ist Silber, Schweigen auch, in: Rademacher/Schmitt-Geiger, Litigation-PR: Alles was Recht ist, Springer 2012, S. 93 ff.*

aa) (Freiwillige) Kommunikation mit der Öffentlichkeit

Interessanter aus Sicht der Datenschutzkommunikation ist der Umgang mit der Datenpanne in der Öffentlichkeit. Die Öffentlichkeit kann zum einen aus eigenem Antrieb gesucht werden, zum anderen besteht aber bei einer großen Zahl von Betroffenen immer das Risiko, dass Dritte über die eigene Datenpanne berichten. In diesem Bereich sind der Kommunikation zumindest aus rechtlicher Sicht wenige Grenzen gesetzt. Hier geht es um die sinnvolle Nutzung von Krisen-PR, die aber innerhalb der Kommunikationswissenschaften nicht unumstritten ist und nicht zuletzt auch vom angestrebten Image des Unternehmens abhängt.

Allerdings sind die eigentlichen Rechtspflichten zur öffentlichen Mitteilung von Datenpannen als solche wenig attraktiv. Die Verantwortlichen Stellen sind deshalb versucht, Eingeständnisse dieser Art auf ein Minimum, das rechtlich Unvermeidbare, zu reduzieren, um den Reputationsverlust gering zu halten. Dennoch raten Öffentlichkeitsarbeiter für Krisen ab einer gewissen Schwere zu Offenheit und Transparenz, um den Vertrauensverlust zu minimieren. – Es gibt also einen Kipppunkt für die Kommunikationsstrategie in diesem Zusammenhang.

Der eigentliche Fehler ist zu diesem Zeitpunkt ohnehin bereits geschehen und nicht mehr aus der Welt zu schaffen. Zu verhindern ist nun, diesen durch falsche oder ungeschickte Kommunikation noch zu verstärken. Dabei ist eine rein juristische Perspektive, die zwangsläufig auf die Verfahrensbeteiligten bezogen und im Kern fachlich und sachlich ist, meist eher hinderlich. Oft wird sogar aus Rechtsgründen eine möglichst restriktive Informationspolitik angeraten. Dies lässt aber die Informationsinteressen der Öffentlichkeit und letztendlich auch die Image-Ziele des Unternehmens außer Acht.

Anders als die möglicherweise beteiligten Juristen muss es gerade Teil der PR-Strategie sein, mit der generellen Öffentlichkeit und den Betroffenen und anderen Interessierten zu kommunizieren. Fasst man die Ziele von PR weiter, so ist hier eine Strategie zur Einflussnahme auf die öffentliche Diskussion und letztlich sogar zur eigenen Reputationskonstitution vonnöten. Ein pauschaler Ratschlag kann insofern ohne Kenntnis der Besonderheiten des Einzelfalles aber kaum abgegeben werden.

Möglicherweise kann sogar die Vermeidung einer öffentlichen Debatte angestrebt werden. Dies ist freilich nur möglich, sofern nicht schon Dritte an die Öffentlichkeit gegangen sind. Dem Vertrauen von Betroffenen, Kunden und dem Image der Verantwortlichen Stelle in der Öffentlichkeit sind an diesem Punkt „No comment"-Aussagen, trotz großer Üblichkeit in der Praxis, selten besonders zuträglich.

Auch droht eine Veröffentlichung des Problems natürlich weiterhin, selbst wenn dieses intern bereits erkannt und eine Vermeidung der Debatte angestrebt wurde. Hier kann eine von Anfang an offensive Strategie einen eigenen Interpretationsrahmen eröffnen und mittelfristig durch Eingestehen des Fehlers und ein Bekennen zu Transparenz eine Reputationsförderung eintreten.

bb) Unternehmensinterne Vorbereitung auf Krisen-Kommunikation

Nicht zu vergessen ist hier die interne Kommunikation mit den eigenen Beschäftigten. Durch die relative Häufigkeit von Datenpannen muss hier schon im Vorfeld eine Vorbereitung auf eine mögliche Krise

stattfinden. Im Hinblick auf den heutigen Stand der Technisierung aller Lebensbereiche ist es realistisch betrachtet kaum zu vermeiden, dass es in einem Unternehmen zu irgendeinem Zeitpunkt zu einer Datenpanne kommen wird.

Die Vorgaben müssen einheitlich und klar sein, damit insbesondere bei überraschender Aufdeckung des Missstandes durch Dritte von Anfang an richtig reagiert werden kann.

Je größer das Unternehmen ist, desto wichtiger wird eine gute organisatorische Aufteilung zwischen Rechts- und PR-Mitarbeitern. Die beste Kommunikationsstrategie kann in so einem Moment durch unklare, nicht abgesprochene und am Ende möglicherweise dadurch widersprüchliche Aussagen aus verschiedenen Teilen des Unternehmens torpediert werden. Gerade bei einer aggressiven, gegebenenfalls sogar im Minutentakt aktualisierten Berichterstattung wird ein immenser Druck aufgebaut, dem nur durch von Anfang an klare Vorgaben sinnvoll begegnet werden kann.

2. Begleitende Kommunikation im Rechtsstreit

a) Vorrang der rechtlichen und rechtsförmigen Kommunikation

Bei Datenschutzverstößen stehen – ebenso wie bei Datenpannen (1.) – optimale rechtliche (rechtsverteidigende) und öffentlichkeitswirksame Kommunikation (PR) in einem Spannungsverhältnis. Weil die rechtlichen Folgen von Datenschutzverstößen erheblich und persönlich (Geldbuße, Geldstrafe, in Ausnahmefällen sogar Haft) sein können, wird hier meist die rechtliche Kommunikationsperspektive im Vordergrund stehen. Aber der sauberste juristische Erfolg kann gleichwohl für Unternehmen oder Behörde als PR-Desaster enden. – Da aber jeder Datenschutz-Krisenfall spezifisch ist, können keine allgemeinen Leitlinien gegeben werden.

b) Datenschutzmediation und ADR

***Schiffer**, Mediation im Datenschutz? in: Conrad/Grützmacher[Hrsg.], Recht der Daten und Datenbanken im Unternehmen, Otto Schmidt-Verlag 2014, S. 1042 ff.*

Eine Möglichkeit, dieses Spannungsverhältnis zwischen allgemeiner Kommunikation und rechtlicher Auseinandersetzung aufzulösen, ist die Alternative Streitbeilegung (Schlichtung, Mediation usw.). In Deutschland, das einen vergleichsweise günstigen Zugang zur Justiz gewährt, haben sich solche Alternativen Streitbeilegungsmechanismen (Alternative Dispute Resolution, ADR) noch nicht überall verbreitet. Trotz der niedrigen Hürden, um vor Gericht zu ziehen, ist die rationale Apathie (s.o.) regelmäßig zu groß und das Datenschutzrecht zu verwickelt, um Konflikte auf diesem Gebiet gerichtsförmig zu klären. Die gerichtlichen Verfahren dienen dabei nicht nur der Durchsetzung von Recht, sondern auch der Klärung der Rechtslage und damit dem allgemeinen Rechtsfrieden wie der individuellen und subjektiven Streitbeilegung.

Diese Befriedungsfunktion bieten auch alternative Streitbeilegungsmechanismen. Sie können (aus Sicht der Verantwortlichen Stelle) rechtliche wie kommunikative Eskalationen – insbesondere den Gang an die Öffentlichkeit – vermeiden helfen. Eine ganze Bandbreite von Ansätzen kommt hier in Frage, von der klassischen Mediation über Schlichtungsverfahren bis hin zu rechnergestützter Online-ADR.

Grundlegende Prinzipien eines Mediationsverfahrens stellen die Freiwilligkeit der Parteien, die Neutralität des Mediators, sowie die Ergebnisoffenheit des Verfahrens dar. Die denkbaren Einsatzmöglichkeiten sind dabei vielfältig. Angefangen von Konflikten innerhalb des Unternehmens, beispielsweise mit dem Datenschutzbeauftragten, über Streitigkeiten mit dem betroffenen Kunden, bis hin zu Konflikten über behördliche Aufsichtsnahmen, ist alles als Gegenstand einer Mediation denkbar.

Einmal kann durch problem- und betroffenenadäquate Verfahren der Bereich rationaler Apathie verringert werden, etwa durch den Einsatz von Formularen. Daneben kann ein bestehender Konflikt aus einer nicht ausschließlich rechtlichen Perspektive gelöst werden, was dann neue Lösungsmöglichkeiten eröffnen kann; in Mediatorenkreisen spricht man diesbezüglich von der „Vergrößerung des Kuchens". Nicht zuletzt scheint auch der Datenschutz durch weite Generalklauseln und viele auslegungsbedürftige und Ermessen eröffnende Vorschriften für die Mediation prädestiniert, was durch den weitgehenden Verzicht auf branchen- oder technologiespezifischen Regelungen in der DSGVO wohl noch verstärkt werden könnte.

Ein Beispiel ist die von der SCHUFA eingerichtete Schlichtungsstelle. Diese privat organisierte ADR – welche seit ihrer Gründung 2010 zuerst mit den Verfassungsrichtern Winfried Hassemer und seit 2014 mit Hans-Jürgen Papier prominent besetzt wurde – versucht nach der erfolglosen Geltendmachung der erhobenen Ansprüche der SCHUFA gegenüber und vor einem Gerichtsverfahren zwischen den beiden Parteien zu vermitteln und so zu einer sachgerechten Lösung zu kommen. Gerade für kleinere Unternehmen sollte aber die Bedeutung einer solchen eigenen Schlichtungsstelle nicht überschätzt werden. So weist der Tätigkeitsbericht der SCHUFA-Schlichtungsstelle für das Jahr 2015 (verfügbar unter http://t1p.de/2xak [SCHUFA, kostenfrei]) lediglich 741 Anträge aus, wobei angegeben wird, dass die SCHUFA zu diesem Zeitpunkt Daten zu 66,4 Mio. Personen gespeichert habe. Im Einzelfall könnte aber die Hinzuziehung eines externen Mediators erwogen werden.

Auch wenn ein offenerer Ansatz offensichtlich Potential und Möglichkeiten bietet, ist durch den vorstehend skizzierten Perspektivenwechsel nur eine graduelle Verbesserung der Datenschutzkommunikation erreichbar.

V. Schluss

Gute Kommunikation muss im Datenschutz insgesamt nicht nur in der Erfüllung der rechtlichen Pflichten bestehen: Es lassen sich durch sinnvolle Nutzung der Instrumente durchaus wettbewerbliche Vorteile generieren und die Verwaltungsleistung optimieren. Nimmt man hierfür die ohnehin verpflichtenden Vorarbeiten als Grundmaterial, so lassen sich in effizienter Weise darauf aufbauend eigene freiwillige Konzepte erstellen.

In den zeitlich folgenden Abschnitten nimmt freilich die Bedeutung der rechtlichen Seite gegenüber der kommunikativen etwas zu, auch hier schafft aber die Datenschutz-Grundverordnung spätestens im Bereich der Haftung und der Sanktionen immer wieder weitere Anreize zu einem überobligatorischen Einsatz.

Selbst für den Krisenfall einer Datenpanne konnte gezeigt werden, dass durchaus Möglichkeiten bestehen, durch sinnvolle Kommunikation eine Ausweitung der Krise einzudämmen und mit Verweis auf eine grundsätzliche Datenschutzfreundlichkeit die anschließenden Bußgeldrisiken zu minimieren.

Der vermeintliche Gegensatz von Rechtspflicht und Kommunikation lässt sich also bei Beachtung der aufgezeigten Grundsätze durchaus bewältigen. Insgesamt lässt sich daher feststellen:

„Gute Kommunikation macht sich bezahlt."

VI. Autoren

Prof. Dr. Kai von Lewinski

lehrt Öffentliches Recht, Medien- und Informationsrecht an der Universität Passau und ist stellvertretender Sprecher des dortigen DFG-Graduiertenkollegs „Privatheit und Digitalisierung“. 2013/2014 war er Wissenschaftlicher Leiter bei der Stiftung Datenschutz.

Dirk Pohl, LL.B. (London)

ist Wissenschaftlicher Mitarbeiter der Forschungsstelle für Rechtsfragen der Digitalisierung (FREDI) an der Universität Passau sowie Wissenschaftlicher Mitarbeiter und Doktorand am Lehrstuhl für Öffentliches Recht, Medien- und Informationsrecht.

Bildnachweise

Anhang

lfd. Nr.	Anbieter	Beschreibung (gemäß Anbieteraussage)	Prüfzeichen	Prüfgrundlagen	Prüfgegenstand: Personen	Prüfgegenstand: Unternehmen / Organisationen	Prüfgegenstand: Prozesse / Systeme	Prüfgegenstand: Produkte / Dienstleistungen	Adressat: Verbraucher	Adressat: Unternehmen	Prüfbedingungen: periodische Zulassung/Re-Zertifizierung	Prüfbedingungen: Selbstbewertung von Produkten für alle Bereiche	Prüfbedingungen: Selbstbewertung von Prüfkriterien mit Zertifizierungsstelle	Prüfbedingungen: Gültigkeitsdauer des Prüfzeichens	Prüfbedingungen: schriftliche Dokumentation + Archivierung erteilter Prüfzeichen	Transparenz: Veröffentlichung der Prüfkriterien	Transparenz: Veröffentlichung der Prüfergebnisse	Erfahrung: Gesamtzahl erteilter Prüfzeichen (Stichtag 01.12.2016)	Erfahrung: öffentliche Liste erteilter Prüfzeichen
1	**ADCERT Privacy Audit GmbH** www.adcert.eu Französische Straße 55 10117 Berlin	Zeichen beschreibt nach prozess- / risikoorientierter Betrachtung Einhaltung der EU-Datenschutzvorgaben. Bewertung und Absicherung geeigneter Datensicherheitsmaßnahmen berücksichtigt jeweilige Kritikalität der Daten. Das Verfahren entspricht - soweit ersichtlich als weltweit einziges Verfahren - vollständig der ISO/IEC 27009:2016 für sektorspezifische Erweiterungen der ISO/IEC 27001 und ist voll EU-DSGVO konform.	**ADCERT - geprüfter Datenschutz**	- Richtlinie 95/46/EG unter Berücksichtigung der Empfehlungen und Stellungnahmen der Art. 29-Gruppe - Datenschutzgrundverordnung (DSGVO) - eigener Kriterienkatalog			x	x		x	ja			x	2 Jahre	ja	nur auf Wunsch		1	ja
2	**Althammer & Kill GmbH & Co. KG** www.althammer-kill.de Neuer Zollhof 3 40221 Düsseldorf	Zertifizierung gemäß Vorgaben mit Vor-Ort-Prüfung, Dokumenten-Review, standardisierten Prüfvorgaben, ggf. Code-Review und Branchen-bezogenen Konretisierungen, z. B. nach § 11 BDSG, Brancheneinsprägung z.B. Gesundheits- und Sozialwesen (auf Basis OH-KIS oder OH-SOZ).	**Zertifizierter Datenschutz**	- Richtlinie 95/46/EG - BDSG, LDSG, TMG, TKG - EU-Datenschutz-Grundverordnung - Orientierungshilfen d. Aufsichtsbehörden - DSG-EKD, KDO, ITSVO-EKD - eigener Kriterienkatalog		x	x	x			x			x	3 Jahre (jährliche Überwachung)	x	ja	auf Kunden-wunsch	k.A.	geplant
		Je nach Prüfauftrag Vor-Ort-Prüfung, Dokumenten-Review, standardisierten Prüfvorgaben und Branchen-bezogenen Konkretisierungen, z. B. nach § 11 BDSG. Brancheneinsprägung beigestellt in Form geprüfter Software im Gesundheits- und Sozialwesen (auf Basis OH-KIS oder OH-SOZ).	**Geprüfter Datenschutz**	- Richtlinie 95/46/EG - BDSG, LDSG, TMG, TKG - EU-Datenschutz-Grundverordnung - Orientierungshilfen d. Aufsichtsbehörden - DSG-EKD, KDO, ITSVO-EKD - eigener Kriterienkatalog		x	x	x			x			x	3 Jahre (jährliche Überwachung)	x	ja	auf Kunden-wunsch	k.A.	geplant
3	**a.k.k. Datenschutz** www.bdsg-externer-datenschutzbeauftragter.de Schulstraße 16a 91245 Simmelsdorf-Hüttenbach	Dokumentation der Datenschutzorganisation im zertifizierten Unternehmen	**a.k.k. companysecure a.k.k. websecure**	- unternehmensindividueller Prüfplan - BDSG, LDSG - BSI IT Grundschutz		x	x			x	nein	x		1 Jahr (ask websecure) 2 Jahre (ask company.)	nein	nein	nein	55	nein
4	**BNT GmbH** www.bntgmbh.de Hauptstr. 73a 66789 St. Leon-Rot	Analyse zur Verbesserung, Umsetzung und Dokumentation datenschutzrelevanter Prozesse im Unternehmen	**Geprüfter Datenschutz**	- BDSG - Richtlinie 95/46/EG - weitere Richtlinien und Gesetze zu Datenschutz und Informationssicherheit		x	x			x	nein	x		1 Jahr	ja	nein	nur auf Kunden-wunsch	k.A.	nein
5	**Check 11 - GDD-Fachgruppe Externe Datenschutzbeauftragte** https://externer-datenschutz.de Am Lerchenhang 21 15299 Müllrorf	Prüfung technischer und organisatorischer Maßnahmen zur Auftragsdatenverarbeitung	**Datenschutzzertifikat Check11**	- § 11 BDSG		x	x			x	nein	x		1 Jahr	ja	Auswahl	nein	23	nein
6	**ConformityTrust GmbH** www.conformitytrust.de Margaretenstraße 48 63225 Langen	Auditierung auf Grundlage der ISO 19011 und Zertifizierung der Konformität zum BDSG und allen weiteren ggf. zutreffenden einschlägigen Regelungen (z. B. TKG, TMG, StGB, SGB, BerufsO u.ä.). Erstellung qualifizierten Auditberichtes inkl. Handlungsempfehlungen und Maßnahmenvorschlägen.	**Trust in Privacy (TIP)**	- BDSG, TKG, TMG, StGB, SGB, Berufsordnungen, usw. - standardisiertes Prüfungsverfahren (DIN EN ISO 19011:2011) - individueller Fragenkatalog		x	x	x	x	x	nein		x	2 Jahre	ja	ja	nein	0	ja

https://stiftungdatenschutz.org/zertifizierung/zertifikate-uebersicht/

lfd. Nr.	Anbieter	Beschreibung (gemäß Anbieteraussage)	Prüfzeichen	Prüfgrundlagen	Prüfgegenstand: Personen	Prüfgegenstand: Unternehmen / Organisationen	Prüfgegenstand: Prozesse / Systeme	Prüfgegenstand: Produkte / Dienstleistungen	Adressat: Verbraucher	Adressat: Unternehmen	Prüfbedingungen: getrennte Zulassung für Prüfung + Zertifizierung	Prüfbedingungen: Einbeziehung von Prüfkriterien für alle Bereiche	Prüfbedingungen: Einbeziehung von Prüfkriterien mit Betriebsgeheimnissen/Zustimmung	Prüfbedingungen: Gültigkeitsdauer des Prüfzeichens	Prüfbedingungen: schriftliche Dokumentation + Archivierung interner Prüfzeichen	Transparenz: Veröffentlichung der Prüfkriterien	Transparenz: Veröffentlichung der Prüfergebnisse	Erfahrung: Gesamtzahl erteilter Prüfzeichen (Stichtag 31.12.2016)	Erfahrung: öffentliche Liste erteilter Prüfzeichen
7	**datenschutz cert GmbH** www.datenschutz-cert.de Konsul-Smidt-Straße 88a 28217 Bremen	Zertifikat zur Auftragsdatenverarbeitung.	**Zertifikat für Auftragsdaten-verarbeitung**	- eigener Kriterienkatalog - BDSG sowie Landes- und Spezialgesetzen zur Auftragsdatenverarbeitung		x	x	x	x	x	ja	x		3 Jahre (jährliche Überwachungs-Audits)		ja	ja	55	ja
		Zertifikat für Datenschutzmanagement	**Zertifikat für Datenschutzmanagementsysteme - privatsm**	- eigener Kriterienkatalog - BDSG sowie Landes- und Spezialgesetzen zur Auftragsdatenverarbeitung		x			x	x	ja	x		3 Jahre (jährliche Überwachungs-Audits)		ja	ja	0	ja
		Vom Bundesverbraucherschutzministerium empfohlenes Zertifikat / Gütesiegel für Webseiten. Eigenes Vorgehen zur Anerkennung von Personen und Prüfstellen.	**Gütesiegel ips – internet privacy standards**	- eigener Kriterienkatalog - rechtliche / IT-sicherheitstechnische Vorgaben zu Daten- und Verbraucherschutz					x	x	ja		x	2 Jahre (halbjährliche Überwachungs-Audits)		ja	ja	230	ja
8	**Deutscher Dialogmarketing Verband e. V.** www.ddv.de Hahnstraße 70 60528 Frankfurt	Nach unabhängiger Vor-Ort-Prüfung werden eines oder mehrere Siegel für Listbroker, Datenveredelung, Lettershop, Fulfillment und/oder Adressverlag vergeben, wenn Datenschutz-anforderungen im Unternehmen einen bestimmten Prozentsatz der Anforderungen erreichen (mehr als 140 Fragen). Siegel erspart Auftraggebern volle Auftragsdatenverarbeitungsprüfung nach § 11 BDSG).	**QuLS-Siegel Listbroker, QuLS-Siegel Datenveredelung, QuLS-Siegel Lettershop, QuLS-Siegel Adressverlag, QuLS-Siegel Fulfillment**	- eigene Kriterienkataloge			x	x			ja		x	Kalenderjahr der Prüfung (jährlich Re-Auditierung 3jährlich Vor-Ort-Prüf.)		ja	ja	114	ja
9	**DQS Deutsche Gesellschaft zur Zertifizierung von Managementsystemen GmbH** www.dqs.de August-Schanz-Straße 21 60433 Frankfurt a. M.	vor-Ort-Prüfung des Datenschutzmanagement-systems auf Konformität mit Maßnahme M 2.501 sowie der organisatorischen und technisch-organisatorischen Maßnahmen mit Anforderungen des Grundschutz-Bausteines B 1.5; zusätzliche Prüfung nach Anhang A von ISO 27001 / 27002 (ggf. auch ISO 27018)	**DQS-Gütesiegel Datenschutz Plus**	- Bausteln B 1.5 BSI-Grundschutz-Katalog - ISO 27001, 27002 - optional: ISO 27018 und Kundenwünsche		x	x				x	x		3 Jahre (jährliches Überwachungs-audit)		ja	ja	k.A.	nein
		vor-Ort-Prüfung des Datenschutzmanagement-systems auf Konformität mit Maßnahme M 2.501 sowie der organisatorischen und technisch-organisatorischen Maßnahmen mit Anforderungen des Grundschutz-Bausteines B 1.5	**DQS-Gütesiegel Datenschutz**	- Bausteln B 1.5 BSI-Grundschutz-Katalog - optional: ISO 27018 und Kundenwünsche		x	x				x	x		3 Jahre (jährliches Überwachungs-audit)		ja	nein		nein
10	**DSZ Datenschutz Zertifizierungs GmbH** www.dsz-audit.de Heinrich-Böll-Ring 10 53119 Bonn	Verfahren richtet sich an Dienstleister aller Branchen, die eine datenschutzkonforme Auftragsdatenverarbeitung gegenüber ihren Kunden anbieten möchten. Datenschutzsiegel tritt neben bestehende Zertifikate wie z.B. nach ISO 27001.	**Datenschutzsiegel**	- § 11 BDSG - eigener Kriterienkatalog (DS-BvD-GDD-01)		x	x	x			ja	x		2 Jahre		ja	ja	3	ja
		Nach technischer und rechtlicher Prüfung und Begutachtung	**ePrivacyseal DE**	- BDSG, TMG, TKG - DSGVO - zusätzliche Anforderungen		x	x	x	x	x	ja	x		2 Jahre		ja	ja	90	ja

lfd. Nr.	Anbieter	Beschreibung (gemäß Anbieteraussage)	Prüfzeichen	Prüfgrundlagen	Prüfgegenstand				Adressat		Prüfbedingungen					Transparanz		Erfahrung	
					Personen	Unternehmen / Organisationen	Prozesse / Systeme	Produkte / Dienstleistungen	Verbraucher	Unternehmen	getrennte Zuständigkeit für Prüfung + Zertifizierung	Einheitskatalog von Prüfkriterien für alle Bereiche	Basiskatalog von Prüfkriterien mit branchenspezif. Zusätzen	Gültigkeitsdauer des Prüfzeichens	schriftliche Dokumentation + Archivierung erhaltener Prüfzeichen	Veröffentlichung der Prüfkriterien	Veröffentlichung der Prüfergebnisse	Gesamtzahl erhaltener Prüfzeichen (Stichtag 31.12.2016)	öffentliche Liste erhaltener Prüfzeichen
11	**ePrivacy GmbH** www.eprivacy.eu Große Bleichen 21 20354 Hamburg	vergebenes Datenschutz-Gütesiegel, das die Einhaltung des eigenen Kriterienkataloges bestätigt, der die Vorgaben des Datenschutzrechts umfasst. Der Schwerpunkt der Datenschutz-Siegel liegt bei elektronischen Produkten, z.B. digitalen Medien, Online-Marketing, Mobile, E-Health usw.	**ePrivacyseal EU**	- EU-Datenschutzrecht inkl. DSGVO - zusätzliche Anforderungen		x	x	x	x	x	ja		x	2 Jahre	ja	ja	ja	20	ja
			ePrivacyseal CH	- Schweizer Datenschutzrecht - zusätzliche Anforderungen		x	x	x	x	x	ja		x	2 Jahre	ja	ja	ja	k.A.	ja
		Zertifizierung im Rahmen des IAB Europe OBA Frameworks. Bei erfolgreicher Zertifizierung Auszeichnung mit europaweit anerkanntem Gütesiegel "EDAA Trust Seal - powered by ePrivacy"	**EDAA OBA Certification**	- IAB Europe OBA Framework			x	x	x	x	ja		x	1 Jahr	ja	ja	ja	100	ja
		Prüfung anhand eines Kataloges mit über 150 Einzelkriterien; bei Apps mit sensiblen Daten wahlweise Zusatzprüfung ePrivacyApp HS mit 60 zusätzlichen Kriterien zu High-Security-Anforderungen	**ePrivacyApp**	eigener Katalog (inkl. BDSG, TMG, EU-Richtlinien, DSGVO, IAB Europe OBA-Framework, Selbstregulierung der Werbewirtschaft etc.)			x	x	x	x	ja		x	Laufzeit geprüfter App-Version	ja	ja	ja	975	ja
12	**editco GbR** www.editco.de Werner-Heisenberg-Straße 5 76829 Landau		**IT-Security- und Datenschutz-Audit**	- BDSG, TMG, StGb, u.ä. - 27000ff, 19001, 9001, 31010 - Standards von BSI, BitKom		x		x	x	x	k.A.	k.A.	k.A.	2 Jahre	k.A:	nein	k.A.	k.A.	nein
13	**EuroPriSe GmbH** www.european-privacy-seal.eu Joseph-Schumpeter-Allee 25 53227 Bonn	Das Siegel beschleunigt die Compliance von IT-Produkten, IT-basierten Diensten (inkl. ADV) und Websites. Nach der Prüfung durch anerkannte rechtliche und technische Gutachter werden die Evaluierungsergebnisse durch eine Zertifizierungsstelle auf Vollständigkeit und Schlüssigkeit geprüft.	**EuroPriSe European Privacy Seal**	- Eigener Anforderungskatalog (online abrufbar) - EU-Datenschutzrecht, insbes. EU-DSGVO - Empfehlungen und Stellungnahmen der EU-Datenschutzaufsichtsbehörden (WP20/Europäischer Datenschutzausschuss)				x	x	x	ja		x (Zusätze bzgl. ePrivacy-Richtlinie)	2 Jahre (Überwachungs-Audits im Abstand von 8 Monaten)	ja	ja	ja	60	ja
		Siegel bestätigt die Vereinbarkeit eines informationstechnischen Produkts mit den Vorschriften über den Datenschutz und die Datensicherheit des Landes Mecklenburg-Vorpommern.	**Gütesiegel Datenschutz M-V**	- § 5 Abs. 2 DSG MV - eigener Prüfkatalog (angelehnt an Katalog des ULD)				x	x	x	ja		x bereichsspezifische Vorschriften des deutschen Rechts (insbes. TMG und TKG)	2 Jahre (Überwachungs-Audits im Abstand von 8 Monaten)	ja	ja	ja	0	ja
14	**GDI Gesellschaft für Datenschutz und Informationssicherheit mbH** www.gdi-mbh.eu Fleyer Straße 61 58097 Hagen	Unabhängige Prüfung aller datenschutzrelevanten Prozesse in einem Unternehmen.	**GDI - zertifizierter Datenschutz**	- BDSG, LDSG - ISO 27001-Anhang 1 (relevante Teile), - BSI-Grundschutz - eigener Kriterienkatalog		x	x	x	x	x	ja	x		1 Jahr (bei Änderungen ggf. abweichend)	ja	nein	nein	157	geplant für Kunden, die das wünschen
15	**GenoTec GmbH** www.geno-tec.de Wilhelm-Haas-Platz 63263 Neu-Isenburg	Unabhängige Dokumentation des Datenschutzniveaus mit Optimierungs-vorschlägen und Testat bei erfolgter Umsetzung. Unterstützung bei der Umsetzung gesetzlicher Vorschriften in effektive und wirtschaftlich vertretbare Verfahrensweisen und Verhaltensregeln.	**Datenschutz-CheckUp mit Zertifikat**	- BDSG, TKG, TMG, UWG, etc. - EU-DSGV	x	x	x	x		x	ja	x		1 Jahr	ja	nein	nur auf Kunden-wunsch	7	nein

https://stiftungdatenschutz.org/zertifizierung/zertifikate-uebersicht/

lfd. Nr.	Anbieter	Beschreibung (gemäß Anbieteraussage)	Prüfzeichen	Prüfgrundlagen	Prüfgegenstand: Personen	Prüfgegenstand: Unternehmen / Organisationen	Prüfgegenstand: Prozesse / Systeme	Prüfgegenstand: Produkte / Dienstleistungen	Adressat: Verbraucher	Adressat: Unternehmen	Prüfbedingungen: gesonderte Zulassungsgebühr für Prüfung + Zertifizierung	Prüfbedingungen: Einbeziehung von Prüfkriterien für alle Bereiche	Prüfbedingungen: Einbeziehung von Prüfkriterien mit Betriebsspezif. Zusätzen	Prüfbedingungen: Gültigkeitsdauer des Prüfzeichens	Prüfbedingungen: Kontrollen: Dokumentation + Archivierung interner Prüfberichte	Transparenz: Veröffentlichung der Prüfkriterien	Transparenz: Veröffentlichung der Prüfungsergebnisse	Erfahrung: Gesamtzahl erteilter Prüfzeichen (Stichtag 31.12.2016)	Erfahrung: Öffentliche Liste erteilter Prüfzeichen
16	**greensagle certification GmbH** www.greensagle-certification.de Beim Strohhause 17 20097 Hamburg	Siegel bescheinigt Konformität von einzelnen Prozessen, IT-Produkten und IT-basierten Dienstleistungen. Geprüft wird anhand der BDSG sowie bereichsspezifischer Spezialgesetze durch anerkannte Sachverständige.	**Datenschutzkonform**	- eigener Anforderungskatalog auf Basis ULD- Prüfkatalog - BDSG, TMG, TKG, UWG etc. - IT-Grundschutz-Kataloge des BSI - Informationssicherheitsmanagement (ISO 27001 und BSI 100-x)		x	x	x			nein		x	2 Jahre	ja	ja	nur auf Kundenwunsch	1	geplant
		Siegel bescheinigt Konformität mit gesetzlichen Vorgaben zur Auftragsdatenverarbeitung inkl. der technischen und organisatorischen Maßnahmen sowie einsätiger bereichsspezifischer Besonderheiten durch anerkannte Sachverständige	**Geprüfte Auftragsdaten-verarbeitung**															
17	**ITR GmbH** www.itr.de Eschenlieder Straße 60c 82194 Gröbenzell	Datenschutz-Status-Analyse zur Umsetzung des betrieblichen Datenschutzes.	**Datenschutz-Status Qualifizierter Datenschutz**	- BDSG - RL 95/46/EG		x	x			x	nein		x	1 Jahr	ja	nein	nur auf Kundenwunsch	k.A.	nein
18	**Institut für organisatorische Informationssysteme - iNOIS** www.inois.de Nosseindia 5 64347 Griesheim	Zertifizierung sollen Anstrengungen im Bereich Datenschutz belegen. Für Zertifizierungen im Bereich Auftragsdatenverarbeitung wird der Prüfkatalog ergänzt bezüglich §§ 9, 11 BDSG. Ein Beirat zur Abstimmung der Prüfkriterien ist vorhanden.	**Zertifizierter Datenschutz + inois Datenschutz-Zertifikat**	- eigener Kriterienkatalog - BDSG, weitere Richtlinien und Gesetze zu Datenschutz und Datensicherheit		x	x				k.A.	k.A.	k.A.	2 Jahre	k.A.	nein	k.A.	k.A.	k.A.
19	**Interev GmbH** www.interev.de Am Pferdemarkt 61a 30853 Langenhagen	Dokumentation der Anwendung von datenschutzrechtlichen Vorgaben im Unternehmen	**Geprüfter Datenschutz durch interev**	- BDSG, LDSG, IDW, GoBD, SGB, TKG, TMG, TDG		x	x	x		x	nein		x	2 Jahre	ja	nein	nein	9	nein
20	**legitimis GmbH** www.legitimis.com Dellbrücker Straße 116 51469 Bergisch Gladbach	Das Prüfzeichen gibt Auskunft über die Einhaltung der für das Unternehmen nach dem Scope der Prüfaussage geltenden und auf es einwirkenden Datenschutzbestimmungen.	**Statement of Compliance**	- unternehmensindividueller Fragenkatalog - BDSG, TMG, TKG, SGB etc. (je nach Anwendbarkeit) - ISO27001, BS10012		x	x			x	nein		x	unbegrenzt (jährliche Überwachung)	ja	nein	nein	3	ja
21	**mediaTest digital GmbH** www.mediatest-digital.com Gosenlecke 4 30159 Hannover	Das Gütesiegel bescheinigt dem App-Anbieter einen sicheren Umgang mit Nutzerdaten durch ausgewogene Datenschutz- und Datensicherheitsprüfung. Zusätzlich werden die AGB und Datenschutzerklärung geprüft. Das Prüfverfahren kann gleichermaßen für Store-Apps und unternehmensinterne Apps verwendet werden.	**TrustedApps**	- eigener Prüfkriterienkatalog (unter Berücksichtigung des BDSG/TMG und der OWASP Mobile Top10)			x				nein	x		1 Jahr	ja	direkt kurzweisen	nur auf Kunden-Wunsch	23	ja

lfd. Nr.	Anbieter	Beschreibung (gemäß Anbieteraussage)	Prüfzeichen	Prüfgrundlagen	Prüfgegenstand				Adressat		Prüfbedingungen					Transparanz		Erfahrung	
					Personen	Unternehmen / Organisationen	Prozesse / Systeme	Produkte / Dienstleistungen	Verbraucher	Unternehmen	getrennte Zuständigkeit für Prüfung + Zertifizierung	Einheitskatalog von Prüfkriterien für alle Bereiche	Basiskatalog von Prüfkriterien mit bereichsspezif. Zusätzen	Gültigkeitsdauer des Prüfzeichens	schriftliche Dokumentation + Archivierung erteilter Prüfzeichen	Veröffentlichung der Prüfkriterien	Veröffentlichung der Prüfergebnisse	Gesamtzahl erteilter Prüfzeichen (Stichtag 31.12.2016)	öffentliche Liste erteilter Prüfzeichen
22	**Privacy Stiftung** www.privacy-stiftung.de Bonner Logsweg 46 53123 Bonn	Das ADV Compliance Audit und das ADV Compliance Siegel als Nachweis über verantwortungsvollen Umgang mit den anvertrauten personenbezogenen Daten richten sich an Auftragsdatenverarbeiter. Für strittige Bewertungsfragen werden Schiedsverfahren angeboten.	**ADV Compliance Checked**	- BDSG - eigener Fragenkatalog		x	(x)	(x)		x	ja	x		3 Jahre (jährliche Kontroll-Audits)	ja	ja	ja	0	ja
24	**Schweizerische Vereinigung für Qualitäts- und Managementsysteme** www.sqs.ch Bernstraße 107 CH-3052-Zollikofen	Zertifiziert werden öffentliche Verwaltungen und private Unternehmen in der Schweiz, Liechtenstein, Österreich und Deutschland. Im Zentrum steht Datenschutz-managementsystem (dazu 80 der 140 Fragen). Der Anbieter ist als seit 1983 weltweit mit eigenen Auditoren tätig; das Gütesiegel befindet sich seit über 10 Jahren auf dem Markt.	**Datenschutzgütesiegel GoodPriv@cy**	- eigener Prüfkatalog - EU-Datenschutzrichtlinie - Anlage 1 zu § 9 BDSG - ISO 9001 und ISO 27001		x		x	x	x	nein	x		3 Jahre (jährliches Überwachungs-Audit)	ja	ja	ja	62	ja
25	**SCHUFA Holding AG** www.schufa.de Kormoranweg 5 65201 Wiesbaden	Zertifizierungsverfahren bezüglich Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Unternehmen und durch Dritte sowie Datensicherheitsmaßnahmen. Zertifizierung bestätigt Implementierung einer Datenschutzorganisation im Unternehmen, Beachtung der Anforderungen zur Datenschutz und Datensicherheit, besonders nach § 9 BDSG.	**SCHUFA -Datenschutz-Siegel**	- eigener Kodex - Gesetze: BDSG, TMG, TKG - Normen: DIN EN ISO 19011:2011	x	x	x	x	x	x	ja	x	x	3 Jahre (jährliche Überwachungs-Audits)	ja	nein	nein	k.A	ja
26	**tacticx gmbH** www.tacticx.de Zeppelinstraße 26 47638 Straelen	Nachweis zur Einhaltung von Datenschutzbestimmungen der ausgewählten Normgrundlage. Darstellung von Datenschutz-konformität und Dokumentation der technischen und organisatorischen Maßnahmen gemäß § 11 BDSG.	**Geprüfter Datenschutz**	- BDSG u. RL95/46/EG - ISO 27001 / BSI-Grundschutz - Katalog ips - internet privacy standards - Katalog EuroPriSe		x	x	x		x	ja		x	unbegrenzt (bis Neubeantragung)	ja	nein	nur auf Kunden-wunsch	k.A.	nein
27	**tekit Consult Bonn GmbH (TÜV Saarland Gruppe)** www.tekit.de Alexanderstraße 10 53111 Bonn	Das Prüfzeichen "Geprüfter Datenschutz" dient als Nachweis für ordnungsgemäß funktionierendes Datenschutzsystem. Es können sowohl Firmen / vollständige Datenverarbeitungsprozesse als auch Teilprozesse zertifiziert werden.	**TÜV Geprüfter Datenschutz TÜV Überwachter Datenschutz**	- BDSG - BSI-Grundschutz (in Teilen); ISO 27001 (wo zutreffend) - Datenschutzcheckliste des TÜV Saarland - branchenspezifische Gesetze, Regelungen, Vertragsklauseln		x	x	x	x	x	ja	x		1 Jahr	Einzel-abfrage über Zert.-datenbank	nein	Einzel-abfrage über Daten-bank	248	Einzel-abfrage über Zertifikats-datenbank
28	**TÜV Informationstechnik GmbH** www.tuvit.de Langemarckstraße 20 45141 Essen	Weiterentwicklung des Gütesiegels aus dem Forschungsprojekt "quid! Das Gütesiegel für Qualität im betrieblichen Datenschutz". Nachweis der Datenschutzkonformität, vorrangig von IT-Verfahren, IT-Produkten, IT-gestützten Diensten. Begutachtung hinsichtlich der materiell-rechtlichen Zulässigkeit der Datenverarbeit., Einhaltung formeller Anforderungen an Datenumgang, Einhaltung von Datenschutzgrundsätzen /Transparenzpflichten/TOMs.	**TÜVIT-Zertifikat Trusted Site Privacy (TSPrivacy)**	- Gesetze: (u.a. BDSG, TMG, TKG) - eigener Kriterienkatalog		x	x	x	x	x	ja	x	x	2 Jahre	ja	ja	ja	20	ja
29	**TÜV Rheinland** www.tuv.com	Zertifikat untersucht, ob Unternehmen Datenschutz- und Datensicherheitsanforderungen für ihren Online Service gerecht wird. Verbindlicher Fragen- u. Verfahrenskatalog unterstützt Know-How-Transfer an internen DSBAusstellung wird durch unabhängige Prüforganisation.	**Datenschutz / Datensicherheit**	- eigener Anforderungskatalog (Grundlage: BDSG sowie Best Practices aus dem Umfeld der Informations- und Datensicherheit wie bspw. ISO 27001 und ISO 18028)		x	x	x		x	ja	x		3 Jahre	ja	nein	nein	22	Einzel-abfrage über Zertifikats-datenbank

https://stiftungdatenschutz.org/zertifizierung/zertifikate-uebersicht/

lfd. Nr.	Anbieter	Beschreibung (gemäß Anbieteraussage)	Prüfzeichen	Prüfgrundlagen	Prüfgegenstand				Adressat			Prüfbedingungen					Transparenz		Erfahrung	
					Personen	Unternehmen / Organisationen	Prozesse / Systeme	Produkte / Dienstleistungen	Verbraucher	Unternehmen	geforderte Zusatzdokumente für Prüfung + Zertifizierung	Einbeziehung/Katalog von Prüfkriterien für alle Bereiche	Einbeziehung/Katalog von Prüfkriterien mit Bereichsspezif. Zusätzen	Gültigkeitsdauer des Prüfkriteriums	Kontrollliste Dokumentation + Archivierung erteilter Prüfzeichen	Veröffentlichung der Prüfkriterien	Veröffentlichung der Prüfungsergebnisse	Gesamtzahl erteilter Prüfzeichen [Stichtag 01.12.2016]	öffentliche Liste erteilter Prüfzeichen
--	Am Grauen Stein 51105 Köln	Zertifikat soll verdeutlichen, dass in dem zertifizierten Unternehmen personenbezogene Daten sicher sind und das Unternehmen vorbildlich in allen Belangen des Datenschutzes ist.	**Geprüfter Datenschutz**	- eigener Anforderungskatalog (Grundlage: BDSG sowie Best Practices aus dem Umfeld des Datenschutzes und zu technisch-organisatorischen Maßnahmen)		x	x			x	ja		x	3 Jahre	ja	nein	nein	9	Einsicht-abfrage über Zertifikats-datenbank
30	**TÜV SÜD sec-IT GmbH** www.tuev-sued.de/sec-it Rodenstraße 65 80339 München	Zertifizierung zum Nachweis von Qualität, Transparenz und Sicherheit, empfohlen von Initiative D21. Die Prüfung von technischen und organisatorischen Anforderungen erfolgt in mehreren Schritten	**TÜV SÜD sg[ten-shopping**	- eigener Anforderungskatalog, angelehnt an Anforderungen aus ISO9001, ISO27001, BDSG, UWG, TMG und anderen			x			x	x		x	unbegrenzt (jährliche Überwachung)	x	ja	nein	220	ja
		Zertifikat unterstützt Auftragnehmer von Auftragsdatenverarbeitungen beim Nachweis der Eignung und Angemessenheit getroffener technisch-organisatorischer Maßnahmen gegenüber Auftraggebern	**Zertifizierte Auftrags-datenverarbeitung**	- eigener Anforderungskatalog, aufbauend auf Anlage zu § 9 BDSG		x	x			x	x		x	1 Jahr (Re-Zertifizierung möglich)	x	ja	nein	5	geplant
31	**Verband für Berater, Sachverständige und Gutachter im Gesundheits- /Sozialwesen e.V.** www.vbsg.org Fohrbachstraße 57 66878 Rodalben	Bescheinigt einer Institution ein ausreichendes/angemessenes Datenschutzniveau entsprechend der vorab definierten personenbezogenen Daten bzw. bestätigt die sichere Auftrags(daten)verarbeitung durch die zertifizierte Stelle unter besonderer Berücksichtigung TOM, an den Vorgaben und Erfordernissen der Europäischen Datenschutzgrundverordnung.	**VBSG-Datenschutzsiegel**	- BDSG, LDSG (soweit relevant) - SGB X - EU-Richtlinie 95/46/EG - BSI-Grundschutz-Kataloge - VBSG-Zertifizierungs-Unterlagen			x	x	x	x	ja		x	3 Jahre	ja	ja	ja	2	ja
30	**Unabhängiges Landeszentrum für Datenschutz** www.datenschutzzentrum.de Holstenstraße 98, 24103 Kiel	Zertifiziert als Datenschutzzuständigkeitsbehörde Inhaltlich datenschutzkonforme IT-Produkte / IT-basierte Dienste (Hardware, Software und automatisierte Verfahren) auf der Grundlage der Datenschutzgütesiegelverordnung (DSGSVO) Schleswig-Holstein.	**ULD-Gütesiegel Datenschutz-Gütesiegel Schleswig-Holstein**	- eigener Anforderungskatalog - Gesetze: (u.a. LDSG, BDSG, TMG, TKG, DSVO)			x	x	x	x	ja			max. 2 Jahre (bei Änderungen ggf. kürzer)	ja	ja	ja	127	ja

STIFTUNG DATENSCHUTZ

Stiftung Datenschutz
rechtsfähige Stiftung bürgerlichen Rechts
Karl-Rothe-Straße 10–14
04105 Leipzig
Deutschland

T 0341 5861 555-0
mail@stiftungdatenschutz.org
www.stiftungdatenschutz.org