Bundesministerium für
Ernährung, Landwirtschaft
und Verbraucherschutz

www.datenschutzzentrum.de

Datenschutz-Auskunftsportal

– Datenschutzrechtliche Aspekte –

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Datenschutz-Auskunftsportal

– Datenschutzrechtliche Aspekte –

Die Förderung des Vorhabens erfolgte aus Mitteln des
Bundesministeriums für Ernährung, Landwirtschaft und Verbraucherschutz (BMELV)
über die Bundesanstalt für Landwirtschaft und Ernährung (BLE)
im Rahmen des Programms zur Innovationsförderung.

Version 1.1

Verfasser:

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein (ULD)
Holstenstr. 98
24103 Kiel

Tel: 0431 988 1200

Mail: mail@datenschutzzentrum.de
www.datenschutzzentrum.de

Inhaltsverzeichnis

1 Einleitung 7
2 Rechtslage 9
2.1 Datenschutzrecht 9
2.1.1 Personenbezogene Daten 9
2.1.2 Betroffene und verantwortliche Stellen 10
2.1.3 Rechtmäßigkeit und „Verbot mit Erlaubnisvorbehalt“ 10
2.1.4 Datensparsamkeitsgrundsatz 10
2.1.5 Erforderlichkeitsgrundsatz 11
2.1.6 Zweckbindungsgrundsatz 11
2.1.7 Datensicherheit 11
2.1.8 Direkterhebungsgrundsatz 11
2.1.9 Grundsatz der Transparenz 12
2.2 Betroffenenrechte im BDSG 13
2.3 Auskunftsrechte 15
2.3.1 Auskunftsrecht gem. § 34 BDSG 16
2.3.2 Authentisierung 18
2.3.3 Auskunftsersuchen und Pseudonyme 20
2.3.4 Zweckbindung der zur Authentisierung übermittelten Daten 21
2.4 Betroffenen- und insbesondere Auskunftsrechte nach dem Entwurf der Europäischen Datenschutz-Grundverordnung 21
2.5 Die Beteiligten – Begriffsbestimmung 23
2.5.1 Anfragende, Auskunftsersuchen, verantwortliche Stelle 23
2.5.2 Auskunftsersuchen mit Auskunftsportal 23
2.5.3 Auskunftsportal 23
3 Problemaufriss: Auskunftsersuchen durch Betroffene 25
3.1 Anlässe für Auskunftsersuchen 25
3.2 Informationsdefizit und Ausführungshindernisse 26
3.3 Ausübung durch Dritte 27
3.4 Eskalationsmöglichkeiten 28
4 Auskunftserteilung durch Unternehmen 30
4.1 Qualität der Auskunft 30
4.1.1 Vollständig 31
4.1.2 Richtig 32
4.1.3 Verständlich 32
4.1.4 Rechtzeitig 33
4.1.5 Qualitätskontrolle 33
4.2 Kosten und Effizienz 34
4.3 Risiken und Rechtsfolgen 34
4.4 Öffentlichkeitswirkung 35
4.5 Optimierung 35
5 Lösungsansatz: Auskunftsportal 36
5.1 Etablierung von Auskunftsprozessen 36
5.2 Grundüberlegungen zu Datenschutzprozessen 37
5.3 Steigerung des Datenschutzniveaus 38
5.4 Ökonomische Gesichtspunkte zum Medienbruch 39
5.5 Zentrale Datenverarbeitung im Portal 40
5.6 Auskunftsportal als unternehmensspezifische Lösung 40

6 Anforderungen an ein Auskunftsportal ... 42
6.1 Allgemeine Anforderungen an ein Auskunftsportal ... 43
6.1.1 Transparenz ... 43
6.1.2 Benutzungsfreundlichkeit ... 44
6.1.3 Informationsangebot eines Auskunftsportals ... 44
6.1.3.1 Unternehmen ... 46
6.1.3.2 Rechtliche Aspekte ... 47
6.1.3.3 Musteranschreiben ... 48
6.1.3.4 Vergabe eines Gütesiegels durch ein Auskunftsportal ... 49
6.2 Auskunftsportal als datenverarbeitende Stelle ... 50
6.2.1 Datenerhebung und -verarbeitung durch das Auskunftsportal ... 50
6.2.1.1 Voraussetzungen ... 50
6.2.1.2 Einwilligung ... 51
6.2.1.3 Erhebung von Nutzungsdaten wie IP-Adressen ... 52
6.2.1.4 Werbung, Optimierung des Dienstes, Statistiken ... 53
6.2.1.5 Bewertungsfunktion ... 55
6.2.1.6 Bezahlsysteme ... 56
6.2.1.7 Speicherdauer ... 57
6.2.1.8 Ort und weitere Vorgaben zur Datenspeicherung ... 58
6.2.2 Datenflüsse ... 59
6.2.2.1 Datenfluss zum Unternehmen ... 59
6.2.2.2 Datenfluss zum Verbraucher ... 60
6.2.3 Technische und organisatorische Anforderungen ... 61
6.2.3.1 Test und Freigabe ... 63
6.2.3.2 Verfahrensdokumentation ... 63
6.2.3.3 Protokollierung ... 64
6.2.3.4 Netzsicherheit ... 65
6.2.3.5 Webhosting ... 66
6.2.3.6 Datenschutzmanagement ... 66
6.3 Vertrauenswürdigkeit des Portals ... 67
6.3.1 Vorbildfunktion des Portals ... 68
6.3.2 Rechtsform des Portals ... 68
6.3.3 Finanzierung ... 69
6.3.4 Interne Kontrollsysteme ... 70
6.3.5 Zertifizierung ... 70
6.3.6 Verantwortungsbereiche der teilnehmenden Unternehmen ... 71
7 Herausforderungen ... 72
7.1 Auskunft über „blanke Daten“ ... 72
7.2 Selbstregulierung ... 73
7.3 Weniger oder mehr Regulierungsbedarf? ... 74
8 Innovative Ansätze und Forschungsfragen ... 76
8.1 Einzelnutzungsnachweise und (elektronischer) Datenbrief ... 76
8.2 Auskunftsersuchen unter Pseudonym ... 77
8.3 Betroffenenunterstützung über ein Identitätenmanagementsystem ... 78
8.4 Ubiquitäre Datenverarbeitung und Wahrnehmung des Auskunftsrechts ... 79
9 Fazit ... 80
Abkürzungsverzeichnis ... 81
Literaturverzeichnis ... 84
Dokumente ... 86

1 Einleitung

Mit zunehmender Digitalisierung nehmen auch die Datenspuren[1] des Einzelnen zu. Über verschiedene Identifikatoren wird eine Verkettung dieser Datenspuren erleichtert. Die Erstellung etwa von Interessenprofilen zur Gestaltung von optimal auf den Empfänger ausgerichteter Werbung wird so ein Leichtes. Der Einzelne hat kaum Möglichkeiten, die Auswertung der von ihm hinterlassenen Datenspuren durch Dritte und die dahinter stehenden Zwecke und Datenströme technisch auszuschließen. Nicht zuletzt weil der Einzelne als Mitglied der Gesellschaft zwangsläufig Daten von sich preisgeben muss. Zudem kann der Einzelne die Verbreitung seiner Daten allerdings auch nicht ohne Weiteres nachvollziehen. Es besteht demnach ein informationelles Ungleichgewicht.[2] Dieses Ungleichgewicht kann etwa durch Auskunftsansprüche vermindert werden. Eine tatsächliche Stärkung der informationellen Selbstbestimmung erfolgt allerdings nur, wenn auch die praktische Umsetzung der Auskunftsansprüche gewährleistet und unterstützt wird.

Die Wahrnehmung des bestehenden und im Datenschutzrecht verankerten Betroffenenrechts auf Auskunft kann durch Auskunftsportale gestärkt werden. Ein Auskunftsportal kann zur effektiven Umsetzung des datenschutzrechtlichen Auskunftsanspruchs beitragen und sowohl Betroffene als auch verantwortliche Stellen wie etwa Unternehmen unterstützen. Es sollte darauf ausgerichtet sein, den Aufwand auf Betroffenenseite bei der Wahrnehmung des Auskunftsrechts zu verringern. Die Unterstützung sollte vor allem darin bestehen, dass Erleichterungen für die Formulierung von Auskunftsersuchen sowie allgemeine Informationen zu Datenschutz und dem Auskunftsrecht zur Verfügung gestellt werden.

Für Betroffene bestehen verschiedene Hindernisse, das datenschutzrechtliche Auskunftsrecht gegenüber verantwortlichen Stellen wahrzunehmen, obwohl Transparenz zu den Grundvoraussetzungen der informationellen Selbstbestimmung gehört und hieran ein zunehmendes öffentliches Interesse besteht. Dies zeigen beispielsweise viele Anfragen und Eingaben bei den Datenschutzaufsichtsbehörden, die sich auf die Form und die Durchführung von Auskunftsersuchen sowie unterbliebene oder unvollständige Auskünfte beziehen. In den zuletzt genannten Fällen haben die verantwortlichen Stellen meist versäumt, einen Prozess zur Auskunftserteilung aufzusetzen. Dadurch entstehen hinsichtlich der zuverlässig korrekten, vollständigen und rechtzeitigen Auskunftserteilung Defizite.

Zwischen Anfragenden und verantwortlicher Stelle nimmt das Auskunftsportal eine zentrale Stellung ein. Da für verantwortliche Stellen hinsichtlich der Erteilung von Auskünften Pflichten, Risiken und Aufwende entstehen, stellen auch sie Anforderungen an ein solches Portal. Die Ausgestaltung eines Portals hat sich daher an der Prämisse zu orientieren, das Auskunftsrecht im Sinne der Be-

[1] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein in Zusammenarbeit mit der Technischen Universität Dresden, Verkettung digitaler Identitäten, Report im Auftrag des Bundesministeriums für Bildung und Forschung; 2007, S. 16 f.

[2] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Erhöhung des Datenschutzniveaus zugunsten der Verbraucher, Studie im Auftrag des Bundesministeriums für Verbraucherschutz, Ernährung und Landwirtschaft, 2006, S. 19 f.

troffenen zu stärken und gleichzeitig die verantwortlichen Stellen zu motivieren, einen Beitrag hierzu zu leisten.

Die folgenden Ausführungen beleuchten zum einen die rechtlichen Rahmenbedingungen des Auskunftsanspruchs sowie „klassische" Problembereiche bei der Umsetzung. Zum anderen wird die Datenverwendung durch ein Auskunftsportal selbst in den Blick genommen. Es wird ein Konzept vorgestellt, das eine zentrale Datenhaltung über das Auskunftsverhalten der Anfragenden im Interesse einer optimalen Umsetzung des Datensparsamkeitsgrundsatzes verhindert und so zusätzliche Risiken für die Betroffenen ausschließt.

Diese Ausarbeitung zu den datenschutzrechtlichen Aspekten eines Datenschutz-Auskunftsportals ist wie folgt strukturiert: Nach dieser Einleitung stellt Abschnitt 2 die Rechslage dar. Abschnitt 3 beschreibt ein Auskunftsersuchen, wie es sich aus Sicht des Betroffenen darstellt. Die Auskunftserteilung durch die verantwortliche Stelle wird in Abschnitt 4 erläutert. Anschließend geht Abschnitt 5 darauf ein, inwieweit ein Datenschutz-Auskunftsportal die aktuelle Situation verbessern könnte. Abschnitt 6 beschreibt detailliert Anforderungen an die Gestaltung und den Betrieb eines solchen Datenschutz-Auskunftsportals. Weitere Herausforderungen, die im Zusammenhang mit solchen Auskunftsportalen diskutiert werden sollten, werden in Abschnitt 7 skizziert. Abschnitt 8 geht über den Stand der Technik hinaus, indem technische Ansätze für erweiterte Lösungen vorgestellt und Forschungsfragen angerissen werden. Schließlich wird in Abschnitt 9 ein Fazit gezogen.

2 Rechtslage

Datenschutz soll den Einzelnen davor schützen, durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt zu werden, § 1 Abs. 1 Bundesdatenschutzgesetz (BDSG). Ziel ist somit nicht nur der Schutz von Daten, sondern der Schutz von Menschen und der sie betreffenden Informationen. Daten über juristische Personen wie Unternehmen fallen nicht unter das Datenschutzrecht, jedoch personenbezogene Unternehmensdaten, z. B. über Kunden oder Beschäftigte.

2.1 Datenschutzrecht

Datenschutz wird in Deutschland grundlegend in dem BDSG und den Datenschutzgesetzen der einzelnen Bundesländer (LDSG) geregelt. Zusätzlich bestehen bereichsspezifische Sonderregelungen beispielsweise im Telemediengesetz (TMG), im Telekommunikationsgesetz (TKG) oder im Sozialgesetzbuch (SGB), die spezielle Bereiche der Datenverarbeitung konkreter regeln. Soweit diese Sonderregelungen Teilaspekte der Datenverarbeitung wie beispielsweise Auskunfts- oder Löschvorgaben nicht regeln, finden wieder die „Auffangvorschriften" des BDSG Anwendung.

Das BDSG setzt die Europäische Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995 (EG-DSRL) um. Derzeit arbeitet die Europäische Kommission an einer Datenschutz-Grundverordnung, deren Entwurf sie am 25. Januar 2012 vorgestellt hat. Mit Inkrafttreten der Verordnung wird eine in der gesamten Europäischen Union unmittelbar anwendbare und somit einheitliche Datenschutzregulierung bestehen. Zu den im Verordnungsentwurf vorgesehenen Betroffenenrechten und insbesondere Transparenzvorgaben vgl. im Einzelnen unten Abschnitt 2.4.

Im BDSG sind bestimmte Grundprinzipien des Datenschutzes festgelegt, die für alle Formen der Datenverwendung Geltung erlangen. Die wesentlichsten Begrifflichkeiten und Grundprinzipien des Datenschutzrechts werden im Folgenden vorgestellt. Betroffenenrechte und der spezielle Transparenzanspruch des § 34 BDSG werden vertieft in den Abschnitten 2.2 und 2.3 dargestellt.

2.1.1 Personenbezogene Daten

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, § 3 Abs. 1 BDSG. Es kann sich also beispielsweise um die Information „Person X ist Hauseigentümer" oder „Angestellter X ist krank" handeln. Als pseudonymisiert gelten Daten gem. § 3 Abs. 6a BDSG, wenn der Name und andere Identifikationsmerkmale durch ein Kennzeichen (beispielsweise eine Nummer) ersetzt wurden, um die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren, also beispielsweise die Information „Angestellter mit der Personalnummer XY ist krank". Ist der Betroffene noch bestimmbar, beispielsweise anhand einer Referenzliste oder Zusatzwissens, so handelt es sich weiterhin um personenbezogene Daten. Als anonymisiert werden Daten angesehen, die derart verändert sind, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können, § 3 Abs. 6 BDSG.

2.1.2 Betroffene und verantwortliche Stellen

Betroffene im Sinne des BDSG sind natürliche Personen, § 3 Abs. 1 BDSG. Das heißt, Betroffene können beispielsweise Verbraucher oder Beschäftigte sein. Unternehmen können keine Betroffenen sein, da sie nicht natürliche, sondern juristische Personen sind. Eine Ausnahme bilden Einzelunternehmen wie beispielsweise eine sogenannte „Ein-Mann-GmbH".

Verantwortliche Stellen im nicht-öffentlichen Bereich können gem. § 2 Abs. 4 BDSG natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts sein. So sind beispielsweise auch Handelsvertreter, Vereine oder Stiftungen erfasst. Verantwortliche Stellen erheben, verarbeiten oder nutzen personenbezogene Daten oder lassen dies durch andere im Auftrag durchführen, § 3 Abs. 7 BDSG.

2.1.3 Rechtmäßigkeit und „Verbot mit Erlaubnisvorbehalt"

Die Verwendung, das heißt die Erhebung, Verarbeitung und Nutzung personenbezogener Daten, ist nur erlaubt, wenn eine Rechtsvorschrift oder eine Einwilligung des Betroffenen es erlaubt, § 4 Abs. 1 BDSG. Das heißt, Datenverwendungen können entweder auf eine Einwilligung des Betroffenen (§ 4a BDSG) gestützt werden oder auf eine gesetzliche Erlaubnis. Datenschutzgesetze enthalten nicht ausschließlich Datenverarbeitungsverbote. Für nicht-öffentliche Stellen wie Unternehmen enthält das BDSG in § 28 und den folgenden Paragraphen Erlaubnisse für bestimmte Datenverwendungen. Ein Unternehmen darf beispielsweise die für die Abwicklung eines Vertrags mit dem Betroffenen erforderlichen Daten erheben, speichern und nutzen. Für eine Versandbestellung betrifft dies üblicherweise den Namen, die Anschrift, den bestellten Artikel und gegebenenfalls die Kontoverbindung des Bestellers. Für die Verwendung dieser Daten benötigt der Versandhändler keine gesonderte Einwilligung des Betroffenen. Eine Speicherung ist so lange zulässig, wie es zur Erreichung des Erhebungszwecks erforderlich ist. Danach müssen die Daten grundsätzlich gelöscht werden. Bestehen nach der Lieferung der Ware aber beispielsweise handels- oder steuerrechtliche Aufbewahrungspflichten, dürfen die erforderlichen Angaben während der Aufbewahrungsfrist gesperrt vorgehalten werden, § 35 Abs. 3 Nr. 1 BDSG. „Gesperrt" bedeutet dabei, dass sie nicht in der aktuellen Kundenkartei gespeichert sind. Die Zulässigkeit der weiteren Verwendung richtet sich nach den konkreten, also beispielsweise handels- oder steuerrechtlichen Aufbewahrungsgründen. Eine Nutzung wäre im letzteren Fall etwa bei einer konkreten Steuerprüfung im Aufbewahrungszeitraum zulässig.

2.1.4 Datensparsamkeitsgrundsatz

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert, § 3a BDSG.

2.1.5 Erforderlichkeitsgrundsatz

Personenbezogene Daten dürfen nur in dem Umfang und für die Dauer erhoben werden, wie es für die Erreichung des vorgesehenen Zwecks erforderlich ist. Für eine Versandbestellung ist beispielsweise die Verwendung des Namens und der Anschrift sowie gegebenenfalls der Kontoverbindung des Bestellers erforderlich. Eine Speicherung ist grundsätzlich nur so lange zulässig, wie es zur Abwicklung der Bestellung erforderlich ist.

2.1.6 Zweckbindungsgrundsatz

Personenbezogene Daten dürfen nur für die Zwecke verwendet werden, für die sie erhoben worden sind, vergleiche beispielsweise § 14 Abs. 1 S. 1 BDSG oder § 28 Abs. 5 BDSG. Die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, sind schon bei der Datenerhebung konkret festzulegen, § 28 Abs. 1 S. 2 BDSG. Eine Verwendung zu einem anderen Zweck ist in der Regel nur zulässig, wenn eine Rechtsvorschrift es erlaubt oder der Betroffene eingewilligt hat. Eine besondere Zweckbindung besteht für personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden. Diese dürfen nach § 31 BDSG nur für die genannten Zwecke verwendet werden.

2.1.7 Datensicherheit

Verantwortliche Stellen müssen gem. § 9 BDSG die technischen und organisatorischen Maßnahmen treffen, die erforderlich sind, um die ordnungsgemäße Ausführung der Datenschutzvorschriften zu gewährleisten. Dabei sind insbesondere Maßnahmen zu treffen, die eine Kontrolle des Zutritts zu Datenverarbeitungsanlagen, des Zugangs zu Datenverarbeitungssystemen, des Zugriffs auf Daten, der Weitergabe, der Eingabe sowie der Verfügbarkeit von Daten, der getrennten Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben worden sind, und der weisungsgemäßen Verarbeitung von Daten, die im Auftrag verarbeitet werden, gewährleisten, vgl. Anlage zu § 9 BDSG.

2.1.8 Direkterhebungsgrundsatz

Der Direkterhebungsgrundsatz stellt ein wichtiges Instrument zur Herstellung von Transparenz für den Betroffenen dar. Personenbezogene Daten sind in der Regel beim Betroffenen zu erheben, § 4 Abs. 2 S. 1 BDSG. Ohne seine Mitwirkung dürfen sie nur im Ausnahmefall erhoben werden, beispielsweise wenn der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder die Erhebung bei dem Betroffenen selbst einen unverhältnismäßigen Aufwand erfordern würde. Eine Ausnahme vom Direkterhebungsgrundsatz kann also beispielsweise bestehen, wenn die Adresse eines unbekannt verzogenen Schuldners ermittelt werden muss, um eine Forderung eintreiben zu können.

2.1.9 Grundsatz der Transparenz

Für den effektiven Schutz der Persönlichkeitsrechte ist es von besonderer Bedeutung, Kenntnis darüber erhalten zu können, von welcher verantwortlichen Stelle zu welchem Zweck welche Daten zu der eigenen Person verwendet werden. Ein allgemeiner Auskunftsanspruch besteht nach § 34 BDSG (vgl. 2.3.1). Aber bereits bei der Erhebung von Daten bei dem Betroffenen ist dieser grundsätzlich über die Identität der verantwortlichen Stelle, den Zweck der Datenverwendung und die Kategorien von Datenempfängern zu informieren, § 4 Abs. 3 BDSG. Bereichsspezifische, teilweise weitergehende Informationspflichten bestehen beispielsweise für Telekommunikationsdiensteanbieter gegenüber Teilnehmern nach § 93 TKG und für Telemedienanbieter gegenüber Nutzern nach § 13 Abs. 1 TMG. Einwilligungen in die Verwendung von Daten sind gem. § 4a Abs. 1 S. 2 BDSG nur wirksam, wenn der Betroffene zuvor ausreichend informiert worden ist. Personenbezogene Daten sind gem. § 4 Abs. 2 BDSG grundsätzlich beim Betroffenen selbst zu erheben (vgl. zum Direkterhebungsgrundsatz im Einzelnen 2.1.8.). Sollte im Ausnahmefall eine Speicherung ohne Kenntnis des Betroffenen stattfinden, ist dieser insbesondere über die Art der Daten, die Zweckbestimmung und die Identität der verantwortlichen Stelle zu benachrichtigen, § 33 Abs. 1 S. 1 BDSG. Speichert eine Stelle personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, also beispielsweise eine Auskunftei, ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen, § 33 Abs. 1 S. 2 BDSG.

Besondere Unterrichtungspflichten treffen gem. § 6c BDSG Stellen, die mobile Speicher- und Verarbeitungsmedien wie Gesundheits- oder Geldkarten mit Prozessorchip ausgeben. Die Unterrichtungspflichten umfassen beispielsweise eine verständliche Darstellung der Funktionsweise des Mediums.

Eine besondere Hinweispflicht besteht gem. § 6b Abs. 2 BDSG auch für Stellen, die öffentlich zugängliche Räume mit optisch-elektronischen Einrichtungen wie Videokameras beobachten. Diese müssen durch geeignete Maßnahmen den Umstand der Beobachtung und die verantwortliche Stelle erkennbar machen. Als geeignet sind beispielsweise deutlich sichtbar angebrachte Schilder oder eindeutige und verständliche Piktogramme[3] anzusehen.

Über das Vorliegen einer automatisierten Einzelentscheidung müssen Betroffene gem. § 6a BDSG informiert werden, wenn diese für ihn rechtliche Folgen nach sich zieht oder eine erhebliche Beeinträchtigung darstellt. Eine ausschließlich auf eine automatisierte Verarbeitung gestützte Entscheidung liegt insbesondere dann vor, wenn keine inhaltliche Bewertung und darauf gestützte Entscheidung durch eine natürliche Person stattgefunden hat. Betroffene können Auskunft über die wesentlichen Gründe der Entscheidung sowie eine Erläuterung verlangen. Der Anspruch auf Auskunft gem. § 34 BDSG erstreckt sich gem. § 6a Abs. 3 BDSG auch auf den logischen Aufbau der automatisierten Datenverarbeitung.

Eine besondere Unterrichtungspflicht besteht gem. § 28b Nr. 4 BDSG, wenn vorgesehen ist, für die Berechnung eines Scorewerts Anschriftendaten des Betroffenen zu nutzen. In diesem Fall besteht eine ausdrückliche Dokumentationspflicht hinsichtlich der Unterrichtung.

---

[3] Wedde in Däubler / Klebe / Wedde / Weichert (Hrsg.), Bundesdatenschutzgesetz Kompaktkommentar, 3. Auflage 2010, § 6b BDSG Rn. 49.

Unternehmen müssen ab einer bestimmten Anzahl von Mitarbeitern, die mit der Verarbeitung personenbezogener Daten beschäftigt sind, oder, wenn sie bestimmte Geschäftsgegenstände wie beispielsweise Adresshandel verfolgen, einen betrieblichen Datenschutzbeauftragten bestellen, § 4f Abs. 1 BDSG. Der betriebliche Datenschutzbeauftragte hat eine Übersicht über die Verfahren der verantwortlichen Stelle jedermann in geeigneter Weise verfügbar zu machen, § 4g Abs. 2 BDSG. Verfahrensübersichten werden auch „Verfahrensverzeichnisse" genannt.

Unternehmen mit bestimmten Geschäftsgegenständen, wie Auskunfteitätigkeit, Adresshandel oder Markt- und Meinungsforschung, haben die Pflicht, Angaben zu den von ihnen betriebenen Verfahren zu dem Register bei der Datenschutzaufsichtsbehörde zu melden, §§ 4d Abs. 1, Abs. 4, 4e BDSG. Das Register kann von jedem eingesehen werden, § 38 Abs. 2 BDSG.

Sind bestimmte besonders gefährdete personenbezogene Daten wie Gesundheits- oder Kontodaten unrechtmäßig Dritten zur Kenntnis gelangt, sind gem. § 42a BDSG unverzüglich die zuständige Datenschutzaufsichtsbehörde sowie die Betroffenen zu informieren. Dies gilt gem. § 15a TMG entsprechend für Anbieter von Telemediendiensten, wenn diese feststellen, dass bei ihnen gespeicherte Bestands- oder Nutzungsdaten unrechtmäßig übermittelt worden oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen des betroffenen Nutzers drohen. Anbieter öffentlich zugänglicher Telekommunikationsdienste haben gem. § 109a TKG im Fall einer Verletzung des Schutzes personenbezogener Daten unverzüglich die Bundesnetzagentur und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit von der Verletzung zu benachrichtigen. Grundsätzlich sind ebenfalls unverzüglich die Betroffenen zu benachrichtigen, wenn anzunehmen ist, dass durch die Verletzung des Schutzes personenbezogener Daten Teilnehmer oder andere Personen schwerwiegend in ihren Rechten oder schutzwürdigen Interessen beeinträchtigt werden. Anbieter von Telekommunikationsdiensten haben ein Verzeichnis der Verletzungen des Schutzes personenbezogener Daten zu führen.

2.2 Betroffenenrechte im BDSG

Im Folgenden werden die wichtigsten Betroffenenrechte des BDSG dargestellt. So sieht das BDSG an verschiedenen Stellen Transparenzrechte vor (vgl. im Einzelnen zum Grundsatz der Transparenz Abschnitt 2.1.9 und zum Auskunftsanspruch nach § 34 BDSG Abschnitt 2.3). Stellt sich heraus, dass unrichtige Daten bei einer Stelle gespeichert sind, so besteht ein Anspruch des Betroffenen auf Berichtigung, § 35 Abs. 1 S. 1 BDSG. Handelt es sich um besondere Arten personenbezogener Daten, § 3 Abs. 9 BDSG, also beispielsweise um Daten zur Religions- oder Parteizugehörigkeit, zum Sexualleben oder zur Gesundheit, oder um Daten über strafbare Handlungen oder Ordnungswidrigkeiten, sind diese zu löschen. Dies gilt für den Fall, dass die Richtigkeit dieser Daten von der speichernden Stelle nicht bewiesen werden kann. In den übrigen Fällen sind Daten bei Meinungsverschiedenheiten über deren Richtigkeit zu sperren. Sperren bedeutet, dass die Daten nicht mehr in dem aktiven Datenbestand, also beispielsweise dem Auskunftsbestand einer Auskunftei, vorhanden sein dürfen. Vielmehr darf ein Zugriff und eine Nutzung der gesperrten Daten technisch-organisatorisch nur für einen bestimmten, gesetzlich vorgesehenen Zweck möglich sein. Die Tatsa-

che der Sperrung darf nicht an Dritte übermittelt werden, § 35 Abs. 4a BDSG. Gesperrt werden müssen auch Daten, die beispielsweise nur noch aufgrund handels- oder steuerrechtlicher Aufbewahrungspflichten vorgehalten werden müssen, § 35 Abs. 3 Nr. 1 BDSG. Zu löschen sind Daten, deren Speicherung unzulässig ist, § 35 Abs. 2 S. 2 Nr. 1 BDSG. Besteht keine Rechtsvorschrift oder Einwilligung des Betroffenen, die eine Speicherung der Daten erlaubt, ist die Speicherung unzulässig und die Daten sind zu löschen. Diese Rechte auf Auskunft gem. § 34 BDSG sowie auf Berichtigung, Löschung und Sperrung gem. § 35 BDSG sind gem.§ 6 Abs. 1 BDSG unabdingbar. Demnach können diese Rechte auch nicht durch Rechtsgeschäft etwa vertraglich durch Allgemeine Geschäftsbedingungen (AGB) ausgeschlossen oder beschränkt werden.

Personenbezogene Daten dürfen zudem nicht automatisiert verarbeitet werden, wenn der Betroffene bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass die schutzwürdigen Interessen wegen seiner besonderen persönlichen Situation die Interessen der verantwortlichen Stelle überwiegen, § 35 Abs. 5 BDSG. Dies gilt allerdings nicht, wenn die verantwortliche Stelle durch eine Rechtsvorschrift zur Verwendung der Daten verpflichtet ist.

Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen gem. § 6a BDSG grundsätzlich nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen. Eine ausschließlich auf eine automatisierte Verarbeitung gestützte Entscheidung liegt insbesondere dann vor, wenn keine inhaltliche Bewertung und darauf gestützte Entscheidung durch eine natürliche Person stattgefunden hat. Eine automatisierte Einzelentscheidung darf ausnahmsweise vorgenommen werden, wenn die Entscheidung im Rahmen eines Vertragsverhältnisses oder eines sonstigen Rechtsverhältnisses ergeht und dem Begehren des Betroffenen stattgegeben wird. Eine Zulässigkeit besteht außerdem ausnahmsweise, wenn die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet, der Betroffene über das Vorliegen einer automatisierten Entscheidung informiert sowie auf Verlangen die wesentlichen Gründe der Entscheidung mitgeteilt und erläutert werden.

Einwilligungen in die Verwendung von Daten gem. § 4a BDSG können in der Regel widerrufen werden. Dies gilt uneingeschränkt für Werbeeinwilligungen beispielsweise hinsichtlich Telefonwerbung. Bestehen gesetzliche Werbebefugnisse wie § 28 Abs. 3 BDSG, steht dem Betroffenen nach § 28 Abs. 4 BDSG ein Widerspruchsrecht zu. Der Widerspruch kann auch gegenüber Stellen wie Auskunfteien oder Adresshändlern erhoben werden, § 29 Abs. 4 BDSG.

Bürgerinnen und Bürger können sich an die Datenschutzaufsichtsbehörden (zu den Zuständigkeiten und Befugnissen vgl. 3.4) wenden, die gem. § 38 BDSG die Ausführung der Vorschriften über den Datenschutz kontrollieren. Zivilrechtlich steht Betroffenen gem. § 7 BDSG ein Schadenersatzanspruch zu, wenn ihnen durch eine unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung ihrer Daten ein Schaden zugefügt wird.

2.3 Auskunftsrechte

Das Recht, Auskunft zu erhalten, ist eine essentielle Voraussetzung für einen effektiven Rechtsschutz. Transparenzansprüche befähigen zur Kontrolle und Durchsetzung weiterer Rechte[4] (zum Grundsatz der Transparenz vgl. 2.1.9). Die deutsche Rechtsordnung kennt auch außerhalb des Datenschutzrechts Auskunftsrechte. So bestehen beispielsweise zivil-, insbesondere handels- und gesellschaftsrechtliche Auskunftsansprüche wie §§ 402, 666, 1379 Bürgerliches Gesetzbuch (BGB), 118, 166 Handelsgesetzbuch (HGB), 51a Gesetz betreffend die Gesellschaften mit beschränkter Haftung (GmbHG), 131Aktiengesetz (AktG). § 83 Betriebsverfassungsgericht (BetrVG) und § 110 Bundesbeamtengesetz (BBG) sehen spezielle Einsichtsrechte in die Personalakte vor. Das deutsche Zivilprozessrecht kennt ein Auskunftsbegehren nach § 142 Zivilprozessordnung (ZPO). So kann ein Gericht anordnen, dass eine Partei oder ein Dritter in seinem Besitz befindliche Urkunden und sonstige Unterlagen, auf die sich eine Partei bezogen hat, vorlegt. Sowohl das materielle als auch das prozessuale deutsche Zivilrecht lassen Auskunftsansprüche allerdings nur im Rahmen dieser besonderen Rechtsgrundlagen zu. Eine allgemeine Auskunftspflicht besteht nicht.[5] In anderen Rechtsordnungen ist dies grundlegend anders strukturiert. So kennt beispielsweise das US-amerikanische außergerichtliche Beweisverfahren im Zivilprozess das Institut der „pretrial discovery". Danach darf von der gegnerischen Prozesspartei die Herausgabe unter anderem von Dokumenten und elektronisch gespeicherten Informationen gefordert werden, die sich in deren oder im Besitz eines Dritten befinden. Vorausgesetzt wird lediglich, dass die Informationen für den Klageanspruch von Relevanz sein könnten. Insgesamt kennt die deutsche Rechtsordnung einen vergleichbar weitgehenden Auskunftsanspruch, auch hinsichtlich Daten mit Drittbezug, nicht.[6]

Außerhalb des Anwendungsbereichs des BDSG können Auskunftsansprüche auch aus § 1004 BGB geltend gemacht werden.[7] Besteht Grund zu der Annahme, dass eine Auskunft unrichtig oder unvollständig erteilt wurde, kann entsprechend §§ 259 Abs. 2, 260 Abs. 2 BGB die Abgabe einer eidesstattlichen Versicherung verlangt werden.[8]

Nach § 13 Abs. 7 TMG hat der Diensteanbieter dem Nutzer nach Maßgabe des § 34 BDSG auf Verlangen Auskunft über die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten zu erteilen. Auf Wunsch des Nutzers kann die Auskunft auch elektronisch erteilt werden. § 93 Abs. 1 S. 4 TKG stellt (deklaratorisch) klar, dass die Auskunftspflicht nach § 34 BDSG für Telekommunikationsdiensteanbieter besteht.

Auskunftsansprüche bestehen auch gegenüber öffentlichen Stellen. Gegenüber öffentlichen Stellen des Bundes, also Bundesbehörden wie dem Kraftfahrt-Bundesamt oder dem Bundesamt für

---

4 Urteil des EuGH vom 07.05.2009, Az. C-553/07 (Rijkeboer), Rn. 51 f.; Urteil des AG Hamburg-Altona vom 17.11.2004, Az. 317 C 338/04, Rn. 21: „Funktion des Auskunftsrechts, dem Betroffenen entscheidungsvorbereitendes Wissen für weiteres Handeln zu vermitteln".

5 Grüneberg in Palandt Bürgerliches Gesetzbuch, 69. Auflage 2010, § 260 Rn. 1.

6 Imberg / Geissl, Dokumentenmanagementrichtlinien und Aufbewahrungspflichten im Hinblick auf die rechtlichen Anforderungen des U.S. Zivilverfahrens, in Corporate Compliance Zeitschrift (CCZ) 2009, S. 190.

7 BGH NJW 22.05.1984, S. 1886; Däubler in Däubler / Klebe / Wedde / Weichert (Hrsg.), Bundesdatenschutzgesetz Kompaktkommentar, 3. Auflage 2010, § 34 BDSG Rn. 57.

8 LG Ulm, Az. 1 S 89/04, 01.12.2004 in DuD 2005, S. 100-103.

Verfassungsschutz, findet § 19 BDSG Anwendung. Grundlegende Fragen, wie etwa der Umfang des Auskunftsanspruchs, sind in dieser Vorschrift wie in § 34 BDSG geregelt. Zu bestimmten Fragen, wie der Ablehnung der Auskunftserteilung, enthält § 19 BDSG dagegen spezielle Vorgaben. Für öffentliche Stellen auf Landesebene, wie Polizei, Kommunalverwaltung oder Schulen, finden die jeweiligen Landesdatenschutzgesetze mit entsprechenden Auskunftsansprüchen Anwendung, z. B. § 27 LDSG Schleswig-Holstein. Außerdem bestehen für bereichsspezifische Sondervorschriften wie § 83 SGB X im Sozialverwaltungsverfahren.

Die speziellen Ansprüche aus Informationsfreiheits- oder Informationszugangsgesetzen betreffen ausschließlich öffentliche Stellen wie Behörden. Zudem bestehen in Verwaltungsverfahren Akteneinsichtsrechte.

2.3.1 Auskunftsrecht gem. § 34 BDSG

Nach § 34 BDSG haben verantwortliche Stellen Auskunft zu erteilen, wenn Betroffene es verlangen. Für das Auskunftsersuchen bestehen keine Formvorgaben. Insbesondere besteht keine Pflicht, das Auskunftsbegehren zu konkretisieren. § 34 Abs. 1 S. 2 BDSG, wonach der Betroffene die Art der Daten, über die Auskunft verlangt wird, näher bezeichnen soll, ist keine Muss- sondern eine Sollvorschrift. Auskunftsbegehren können vom Betroffenen auf einzelne Fragen beschränkt werden. Betroffene haben allerdings auch die Möglichkeit, allgemein nach allen zu ihrer Person gespeicherten Daten zu fragen.

Der Anspruch kann geltend gemacht werden, auch wenn Anfragende sich nicht sicher sind, ob zu ihrer Person Daten bei der verantwortlichen Stelle gespeichert sind. Die Vorlage zu § 34 BDSG, Art. 12 a) EG-Datenschutzrichtlinie (95/46/EG), stellt hierzu klar, dass eine Bestätigung zu erfolgen hat, ob zur Person des Anfragenden Daten verarbeitet werden oder nicht.

Die verantwortliche Stelle hat zu informieren, welche Daten zu dem Anfragenden zu welchem Zweck gespeichert werden. Sie muss auch mitteilen, aus welchen Quellen die Daten stammen und an welche Empfänger oder Kategorien von Empfängern die Daten weitergegeben werden. Empfänger sind gem. § 3 Abs. 8 BDSG keine Dritten und erfassen demnach auch Stellen innerhalb des Verantwortungsbereichs der verantwortlichen Stelle, wie etwa Auftragsdatenverarbeiter (vgl. §§ 3 Abs. 7, 11 BDSG). Werden Daten zu Zwecken der Werbung gem. § 28 Abs. 3 S. 4 BDSG übermittelt, besteht gem. § 34 Abs. 1a BDSG die Pflicht, die Herkunft der Daten und die konkreten Empfänger für die Dauer von zwei Jahren zu speichern, um Auskunft erteilen zu können. Nach der Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH)[9] muss auch im Übrigen das Recht, Auskunft über Empfänger oder Kategorien von Empfängern zu erhalten, zwingend die Vergangenheit erfassen, um Sinn und Zweck des Auskunftsanspruchs zur Geltung zu verhelfen. Hieraus folgt eine Pflicht, Empfänger oder Kategorien von Empfängern sowie die an sie übermittelten Daten zu speichern, um Auskunft erteilen zu können. Für die Speicherfrist kann die zulässige Aufbewahrungsdauer der übermittelten Daten eine Orientierung bieten.[10] Die EG-Datenschutzrichtlinie verlange

[9] Urteil des EuGH vom 07.05.2009, Az. C-553/07 (Rijkeboer), Rn. 54.

[10] Urteil des EuGH vom 07.05.2009, Az. C-553/07 (Rijkeboer), Rn. 58.

allerdings keine unverhältnismäßige Belastung, die etwa eintreten könne, wenn die Frequenz der Übermittlungen an eine geringere Zahl von Empfängern hoch sei. Da der deutsche Gesetzgeber abgesehen von § 28 Abs. 3 S. 4 BDSG keine Speicherfrist festgelegt hat, haben verantwortliche Stellen selbst eine interessengerechte Speicherdauer vorzusehen, die eine adäquate Wahrnehmung des Auskunftsrechts[11] ermöglicht.

Stellen, die personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung speichern, also beispielsweise Auskunfteien oder Adresshändler, haben Auskünfte auch dann zu erteilen, wenn sie beispielsweise personenbezogene Daten zu dem Anfragenden nicht selbst speichern, aber zur Erfüllung von Werbeaufträgen Datenbestände anderer Stellen nutzen, § 35 Abs. 3 S. 2 Nr. 2 BDSG. Außerdem müssen diese Stellen Auskunft über die zu einer Person gespeicherten Daten auch dann erteilen, wenn die Daten weder automatisiert verarbeitet werden noch in einer nicht automatisierten Datei gespeichert sind, § 35 Abs. 3 S. 1 BDSG. Betroffene können von diesen Stellen auch Auskunft über Daten verlangen, die zum Zeitpunkt des Auskunftsersuchens noch keinen Personenbezug aufweisen, bei denen ein solcher aber im Zusammenhang mit einer Übermittlung an einen Dritten hergestellt werden soll, § 35 Abs. 3 S. 2 Nr. 1 BDSG.

Für den Fall der Berechnung von Wahrscheinlichkeitswerten, die auch Scorewerte genannt werden, bestehen besondere Auskunftsrechte. Diese bestehen zum einen nach § 34 Abs. 2 BDSG gegenüber der für die Entscheidung verantwortlichen Stelle, wie etwa einem Kreditinstitut, das selbst ein Scoringverfahren durchführt. Besondere Auskunftsrechte bestehen zum anderen gem. § 34 Abs. 4 BDSG aber auch gegenüber Stellen, die geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung verarbeiten, wie z. B. Kreditauskunfteien. Insbesondere muss eine einzelfallbezogene und nachvollziehbare Erklärung des Zustandekommens und der Bedeutung des Wahrscheinlichkeitswerts in allgemein verständlicher Form erteilt werden. Im Falle von automatisierten Entscheidungsverfahren ohne die inhaltliche Bewertung durch eine natürliche Person erstreckt sich der Anspruch auch auf den logischen Aufbau der Datenverarbeitung, § 6a BDSG. Außerdem kann der Anspruch bestehen, unaufgefordert über das Vorliegen einer automatisierten Entscheidung informiert zu werden. Auf Verlangen sind dann die wesentlichen Gründe der Entscheidung zu erläutern.

Die Auskunft kann gem. § 34 Abs. 6 BDSG in Textform verlangt werden. Gem. § 126b BGB muss die Erklärung demnach in einer Urkunde oder auf andere zur dauerhaften Wiedergabe in Schriftzeichen geeignete Weise abgegeben, die Person des Erklärenden genannt und der Abschluss der Erklärung durch Nachbildung der Namensunterschrift oder anders erkennbar gemacht werden. Die Auskunft muss gem. § 34 Abs. 8 BDSG vorbehaltlich von Ausnahmen unentgeltlich erteilt werden. Stellen, die geschäftsmäßig Daten zum Zweck der Übermittlung speichern, wie Auskunfteien, müssen nur einmal je Kalenderjahr eine unentgeltliche Auskunft erteilen, wenn Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen können. Das Entgelt darf über die unmittelbar zurechenbaren Kosten nicht hinausgehen. Natürlich bleibt es den Unternehmen unbenommen, aus Kulanz auch weitere Auskünfte in einem Kalenderjahr kostenfrei zu erteilen. Ein Entgelt darf auch bei Vorliegen der oben genannten Voraussetzungen nicht erhoben werden, wenn be-

[11] Urteil des EuGH vom 07.05.2009, Az. C-553/07 (Rijkeboer), Rn. 57.

sondere Umstände die Annahme rechtfertigen, dass Daten unrichtig oder unzulässig gespeichert werden, oder wenn eine Auskunft ergibt, dass die gespeicherten Daten zu berichtigen oder zu löschen sind. Ist die Auskunft nicht unentgeltlich, muss darauf hingewiesen werden, dass die Möglichkeit besteht, sich persönlich Kenntnis über die betreffenden Daten zu verschaffen.

§ 34 BDSG findet Anwendung gegenüber nicht-öffentlichen Stellen. Das sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, § 2 Abs. 3 BDSG. In der Praxis erlangt § 34 BDSG vor allem gegenüber Unternehmen Bedeutung. Gegenüber öffentlichen Stellen des Bundes, also Bundesbehörden wie dem Kraftfahrt-Bundesamt oder dem Bundesamt für Verfassungsschutz, findet der § 19 BDSG Anwendung. Für öffentliche Stellen auf Landesebene, wie Polizei, Kommunalverwaltung und Schulen, finden die jeweiligen Landesdatenschutzgesetze mit entsprechenden Auskunftsansprüchen Anwendung. Außerdem bestehen für besondere Bereiche Spezialvorschriften wie § 83 SGB X im Sozialverwaltungsverfahren.

2.3.2 Authentisierung

Personenbezogene Daten dürfen generell nicht an unberechtigte Dritte übermittelt werden.[12] Eine Auskunft nach § 34 BDSG enthält zwangsläufig personenbezogene Daten. Sie enthält in der Regel sogar einen Gesamtüberblick über die zu einer Person bei einer Stelle gespeicherten Daten. Bereits aufgrund dieser Konzentration sind die Angaben besonders schutzwürdig. Zudem handelt es sich regelmäßig um in einer bestimmten Form verifizierte und somit besonders aussagekräftige Daten. Anfragende müssen eindeutig als zum Erhalt der Auskunft Berechtigte identifiziert werden. Maßgaben für die Identifizierung sind nicht ausdrücklich gesetzlich geregelt. Aus den datenschutzrechtlichen Grundsätzen wie dem Erforderlichkeitsgrundsatz (vgl. 2.1.5) ergibt sich, dass Anfragende nur die Informationen zu ihrer Person angeben müssen, die für die verantwortliche Stelle zur Identifizierung der anfragenden Person in ihrem Datenbestand erforderlich sind. Für die Identifizierung erforderlich sind in der Regel Name, Anschrift und Geburtsdatum. Die Erforderlichkeit richtet sich aber generell nach den Referenzdaten, die in einer Organisation vorhanden sind. So kann statt des Geburtsdatums beispielsweise eine Vertragsnummer erforderlich sein zur Identifizierung, falls die Strukturierung der Kundendatensätze nur mit Hilfe dieses Datums erfolgt. Anhand von Namen und Anschrift kann jedenfalls im postalischen Verfahren sicher eine Auskunft an den Betroffenen erteilt werden. Ist der Betroffene mit der Anschrift im Datenbestand der verantwortlichen Stelle gespeichert, kann davon ausgegangen werden, dass anhand der genannten Daten nur dem tatsächlich Betroffenen die Auskunft erteilt wird, selbst wenn eine andere Person als der Betroffene das Auskunftsersuchen – im fremden Namen – gestellt haben sollte. Weitere Datenkategorien wie der Geburtsort dürfen nur erhoben werden, wenn die zuvor genannten Daten zur Identifizierung nicht ausreichen und bei der verantwortlichen Stelle ein entsprechendes Referenzdatum vorhanden ist. Die Erhebung der Daten zur Identifizierung dient allein dem Zweck der Verhinderung einer Übermittlung von Daten an unberechtigte Dritte (zur Zweckbindung vgl. 2.3.4). Kann die Stelle den Anfragenden anhand der übermittelten Daten eindeutig identifizieren, ist keine weitere Erhebung von Daten erforderlich. Dies ist insbesondere der Fall, wenn in einem engen zeitlichen Zusammen-

[12] Vgl. § 43 Abs. 2 Nr. 1 BDSG.

hang Schriftverkehr wie eine Benachrichtigung nach § 33 BDSG stattgefunden hat. Eine Erhebung weiterer Identifikationsdaten ist regelmäßig auch dann nicht erforderlich, wenn anhand der übermittelten Daten jedenfalls feststeht, dass keine Daten zu dem Betroffenen bei der verantwortlichen Stelle gespeichert sind. Nur dieser Umstand wird in diesem Fall beauskunftet. Er wird in der Regel nicht als besonders schützenswert einzustufen sein. Hat die Information, nicht in einer Datei – beispielsweise für potentielle Führungskräfte – gespeichert zu sein, allerdings einen Aussagegehalt, muss dies bei der Auskunftserteilung und der Intensität der Identifizierung berücksichtigt werden.

Kann die Stelle den Anfragenden anhand der übermittelten Identifikationsdaten nicht eindeutig identifizieren, weil beispielsweise Namensvetter mit derselben Anschrift, zum Beispiel in großen Wohneinheiten oder Hans Maier Junior und Hans Maier Senior, gespeichert sind, müssen weitere Identifizierungsdaten erhoben werden. Geeignet könnte zur Identifizierung in den genannten Beispielen das Geburtsdatum sein, sofern ein entsprechendes Referenzdatum im Datenbestand der verantwortlichen Stelle vorhanden ist. Verantwortliche Stellen wie Auskunfteien, die geschäftsmäßig Auskünfte auch an Dritte erteilen, müssen bei dem Aufbau des Datenbestandes berücksichtigen, dass Personenverwechslungen generell unterbunden werden müssen.

Von verantwortlichen Stellen wie Auskunfteien wird häufig angeführt, um Personenverwechslungen und Identitätsmissbrauch zu vermeiden, sei die Vorlage einer Personalausweiskopie generell erforderlich. Sie diene beispielsweise der Vermeidung von Manipulationen mit dem Ziel, die „einwandfreie Auskunft" zu erhalten, „keine (negativen) Daten gespeichert", die durch geringfügige Änderungen der tatsächlichen Identitätsdaten unternommen würden.[13] Es stellt sich die Frage, ob in spezifischen Zweifelsfällen Ausweiskopien geeignet sind, Anfragende eindeutig im Datenbestand zu identifiziert. Mit der absehbaren Verbreitung des neuen Personalausweises (nPA) werden sich diesbezüglich ohnehin Änderungen ergeben. § 14 Personalausweisgesetz (PAuswG) stellt laut der Gesetzesbegründung[14] klar, dass die Erhebung und Verwendung personenbezogener Daten aus oder mithilfe des Ausweises künftig nur über die dafür vorgesehenen Wege erfolgen darf. Dies sind für nicht-öffentliche und öffentliche Stellen der elektronische Identitätsnachweis und für zur hoheitlichen Identitätsfeststellung berechtigte Behörden der Abruf der elektronisch gespeicherten Daten einschließlich der biometrischen Daten. Weitere Verfahren z. B. über die opto-elektronische Erfassung („Scannen") von Ausweisdaten oder den maschinenlesbaren Bereich sollen ausdrücklich ausgeschlossen werden. Die Verwendung einer Kopie ist somit – wenn überhaupt – nur bei Einsatz des herkömmlichen Personalausweises denkbar. Auch in diesem Fall dürfen durch die Kopie allerdings keinesfalls mehr Daten erhoben werden, als der Anfragende bei der Beantragung der Auskunft selbst mitteilt. Die Ausweiskopie soll nur der Verifizierung der angegebenen Identifizierungsdaten dienen. Bis auf die Angaben zu Name, Anschrift, Geburtsdatum können Personalausweiskopien für diesen Zweck geschwärzt werden. Denn darüber hinausgehende Informationen wie Grö-

[13] Eine weitere Frage ist, für welche Zwecke Eigenauskünfte genutzt bzw. verlangt werden dürfen. Jedenfalls die Forderung von Vermietern nach der Vorlage der (umfangreichen) Eigenauskunft des potentiellen Mieters ist datenschutzrechtlich unzulässig. Vgl. Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) vom 22.10.2009, „Bonitätsauskünfte über Mietinteressenten nur eingeschränkt zulässig". https://www.datenschutz.de/aufsicht_privat/ (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

[14] Bundesrat-Drucksache 550/08, S. 69 f., 08.08.2008.

ße, Augenfarbe und Personalausweisnummer sind nicht geeignet und erforderlich zur Identifizierung durch eine nicht-öffentliche Stelle.

Personalausweiskopien können auch nicht mit dem Argument pauschal vom Anfragenden angefordert werden, sie würden ein geeignetes Mittel zur Vermeidung missbräuchlicher Auskunftsersuchen darstellen. Dies gilt selbst dann, wenn dies als eine gewisse Hürde angesehen würde, die nur durch kriminellen Aufwand überwunden werden kann. Denn die Fälschung einer Personalausweiskopie ist technisch beispielsweise mit Bildbearbeitungssoftware möglich. Daher können Personalausweiskopie nur als bedingt sicheres und damit nur bedingt geeignetes Mittel zur Vermeidung von Identitätsmissbrauch angesehen werden.

Bestehen Zweifel an der Identität des Anfragenden und können diese auf anderem Wege nicht ausgeräumt werden, kann eine beglaubigte Unterschrift zum Nachweis der Identität verlangt werden.[15] Derart hohe Anforderungen dürfen aber nur gestellt werde, wenn es im Einzelfall erforderlich ist. Im Übrigen darf die Wahrnehmung von Betroffenenrechten nicht durch unangemessen hohe Voraussetzungen vereitelt werden.

2.3.3 Auskunftsersuchen und Pseudonyme

Lassen pseudonymisierte Daten eine Bestimmung der betroffenen Person zu, handelt es sich um personenbezogene Daten gem. § 3 Abs. 1 BDSG. Für diese findet der Auskunftsanspruch des § 34 BDSG Anwendung.[16] Die Möglichkeit der Wahrnehmung der Betroffenenrechte im Fall der Verwendung pseudonymisierter Daten ist angezeigt, da beispielsweise über Verknüpfungen verschiedener Datensätze ebenfalls Gefahren für die Persönlichkeitsrechte der Betroffenen drohen. Das TMG greift dies in § 13 Abs. 7 auf, indem es Diensteanbieter ausdrücklich zur Auskunftserteilung über die zu einem Pseudonym gespeicherten Daten verpflichtet.

Das Verfahren der Auskunftserteilung, insbesondere das Beantragen einer Auskunft unter Pseudonym, stellt für die verantwortliche Stelle eine Herausforderung dar. Die Regelung des § 13 Abs. 7 i. V. m. Abs. 6 TMG setzt eine solche Auskunftserteilung allerdings voraus. Denn sofern es technisch realisierbar ist, hat der Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen. Diese Vorgabe würde konterkariert, wenn zur Geltendmachung von Betroffenenrechten weitergehende Daten erhoben werden dürften. Dies gilt auch außerhalb des Anwendungsbereichs des TMG für den Fall der Verwendung von Pseudonymen. Denn Pseudonymisierung ist eine Maßnahme der Datensparsamkeit gem. § 3a BDSG. Der Grundsatz der Datensparsamkeit muss in allen Stadien des Datenumgangs sichergestellt sein und darf nicht gerade in dem Fall der Geltendmachung von Betroffenenrechten unterlaufen werden. Vielmehr müssen Strukturen geschaffen werden, die eine Auskunftserteilung unter Pseudonym ermöglichen.

---

[15] Dix in Simitis (Hrsg.), Kommentar zum BDSG, 7. Auflage 2011, § 34 BDSG Rn. 43.

[16] Zu Betroffenenrechten im Allgemeinen: Weichert in Däubler / Klebe / Wedde / Weichert (Hrsg.), Bundesdatenschutzgesetz Kompaktkommentar, 3. Auflage 2010, § 3 BDSG Rn. 51, mit Nachweis zu a. A..

Dies kann etwa durch die Vereinbarung eines Kennsatzes[17] oder eines Passworts für die Auskunftsbeantragung beispielsweise im Rahmen eines Anmeldeprozesses gewährleistet werden.

2.3.4 Zweckbindung der zur Authentisierung übermittelten Daten

Daten, die Anfragende zum Zweck der Auskunftserteilung nach § 34 BDSG gegenüber einer verantwortlichen Stelle angeben, dürfen gem. § 34 Abs. 5 BDSG nur für diesen Zweck sowie den Zweck der Datenschutzkontrolle verwendet werden. Es ist daher insbesondere nicht zulässig, mit diesen Daten den allgemeinen Datenbestand einer angefragten Stelle, wie beispielsweise den Auskunftsbestand einer Auskunftei, zu befüllen und die Daten für eigene Zwecke der Stelle zu nutzen. Der Umstand, dass eine Person Betroffenenrechte wahrnimmt, darf daher auch keinesfalls als Bewertungskriterium beispielsweise in Scoringverfahren verwendet werden.

2.4 Betroffenen- und insbesondere Auskunftsrechte nach dem Entwurf der Europäischen Datenschutz-Grundverordnung

Kapitel 3 des Entwurfs der Europäischen Datenschutz-Grundverordnung (E-EU-DSGVO) sieht Regelungen hinsichtlich der Rechte der Betroffenen vor. Die einzelnen Abschnitte treffen insbesondere Vorgaben zu Transparenz, Informationspflichten und Auskunftsrechten, Berichtigung und Löschung sowie Widerspruchsrechten und Profiling. Die fundamentale Neuerung des Verordnungsentwurfs besteht in diesem Zusammenhang in der grundlegenden Regelung des Kommunikationsverhältnisses zwischen der verantwortlichen Stelle und den Betroffenen.

So ist vorgesehen, dass die verantwortliche Stelle nach Art. 11 der E-EU-DSGVO in Bezug auf die Verarbeitung personenbezogener Daten und die Ausübung der den betroffenen Personen zustehenden Rechte eine nachvollziehbare und für jedermann leicht zugängliche Strategie verfolgen soll. Dem Betroffenen sollen alle Informationen und Mitteilungen zur Verarbeitung personenbezogener Daten in verständlicher Form unter Verwendung einer klaren, einfachen und adressatengerechten Sprache zur Verfügung gestellt werden. Dies soll insbesondere dann gelten, wenn die Informationen an ein Kind gerichtet werden.

Nach Art. 12 E-EU-DSGVO soll die verantwortliche Stelle Verfahren etablieren, mittels derer sie den Betroffenen Informationen zur Herstellung von Transparenz bei der Erhebung von Daten bereitstellt und die Ausübung ihrer Rechte wie dem Auskunfts-, Berichtigungs- und Löschungsanspruch ermöglicht. Es sollen explizit Vorkehrungen getroffen werden, um die Wahrnehmung der Rechte zu erleichtern. Diese Vorgabe sagt zum einen aus, dass die Wahrnehmung der Betroffenenrechte nach dem derzeitigen Stand als zu beschwerlich empfunden wird. Zum anderen wird die Verantwortung dafür und für eine Verbesserung der Situation nicht allein den Betroffenen aufgeladen. Vielmehr wird eine Zielvorgabe an die verantwortlichen Stellen gemacht: Diese müssen aktiv Vorkehrungen treffen und diese müssen für die Wahrnehmung der Betroffenenrechte eine Erleichterung bewirken.

[17] Dix in Simitis (Hrsg.), Kommentar zum BDSG, 7. Auflage 2011, § 34 BDSG Rn. 45.

Im Falle der automatischen Verarbeitung personenbezogener Daten soll nach Art. 12 E-EU-DSGVO auch die elektronische Beantragung der Rechte ermöglicht werden. Diese Vorgabe soll der Technisierung des Alltags und den modernen Kommunikationsgewohnheiten Rechnung tragen.

Der E-EU-DSGVO macht in Art. 12 eine klare Vorgabe zu der Frist, innerhalb derer Auskünfte erteilt werden müssen. Die Frist beträgt grundsätzlich einen Monat. Stellt der Betroffene den Antrag in elektronischer Form, hat die Antwort auf elektronischem Weg zu erfolgen, sofern er nichts anderes angibt. Auch hier stellen sich in weiten Bereichen Fragen nach der sicheren Identifikation des Betroffenen.

Die Auskunft soll grundsätzlich unentgeltlich bleiben. Für den Fall von „offenkundig unverhältnismäßigen Anträgen" wird den verantwortlichen Stellen – unabhängig von der Branche – die Möglichkeit eingeräumt, ein Entgelt zu erheben oder keine Auskunft zu erteilen. Die Regelung wirft aufgrund ihrer Unbestimmtheit Zweifel an ihrer Eignung zur Herstellung von Rechtsklarheit auf. Die Kommission räumt sich allerdings die Ermächtigung ein, die Kriterien und Voraussetzungen für offenkundig unverhältnismäßige Anträge zu regeln. Dass der bloße Umstand der Häufung von Anfragen aber als unverhältnismäßig gewertet werden und damit die verantwortliche Stelle berechtigen kann, keine Auskunft zu erteilen, lässt grundlegende Zweifel an einer Eignung der Regelung zu einem angemessenen Ausgleich der Interessen auftreten. Denn eine Häufung kann auch auftreten, wenn legitimer Weise die Richtigkeit des Datenbestands einer verantwortlichen Stelle kontrolliert, Fehler festgestellt und die Berichtigung kontrolliert wird.

Die Informationspflicht zur Herstellung von Transparenz bei der Erhebung von Daten wird gegenüber dem derzeitigen Stand ausgeweitet, Art. 14 E-EU-DSGVO. So soll beispielsweise auf die Kategorien personenbezogener Daten, die allgemein verarbeitet werden, hingewiesen werden müssen. Betroffenen können so einen Eindruck von dem Kontext erhalten, in dem ihre Daten verwendet werden. Es müssen zudem diejenigen personenbezogenen Daten beauskunftet werden, die Gegenstand der Verarbeitung sind, sowie alle verfügbaren Informationen über die Herkunft der Daten. Eine besondere Neuerung könnte darin bestehen, dass zumindest im Fall von „Profiling" über die Tragweite der Verarbeitung und die mit ihr angestrebten Auswirkungen Auskunft erteilt werden muss. Mit Blick auf die derzeitigen Auskunftsansprüche zu Scoring nach § 34 Abs. 2 und 4 BDSG ist allerdings eine ernüchternde Umsetzung zu befürchten.

Bestehen bleiben soll das Recht, Berichtigung unzutreffender personenbezogenen Daten zu verlangen. Derzeit ist die Berichtigungspflicht allerdings in § 35 Abs. 1 BDSG als Grundsatz ausgestaltet, die keiner Geltendmachung bedarf, und erscheint insofern als für den Betroffenen vorteilhafter. Betroffene sollen zudem das Recht erhalten, die Vervollständigung unvollständiger personenbezogener Daten verlangen zu können. Dies setzt die Kenntnis voraus, wann ein Datensatz als vollständig angesehen wird. Des Weiteren setzt es aber auch die Kenntnis darüber voraus, wie bestimmte Informationen und wie „Datenlücken" von der verantwortlichen Stelle beurteilt werden, welchen Einfluss sie insbesondere auf Wahrscheinlichkeits- bzw. Scorewertberechnungen haben.

Art. 17 E-EU-DSGVO sieht das Recht auf Löschung vor. Außerdem soll eine „Präzisierung" in Form eines Rechts auf Vergessenwerden eingeführt werden. Hierzu soll die Pflicht der verantwortlichen Stelle, die personenbezogene Daten veröffentlicht hat, gehören, Dritte über den Antrag des Be-

troffenen auf Löschung aller Verbindungen zu diesen personenbezogenen Daten oder auf Löschung von Kopien oder Replikationen dieser Daten zu informieren. Das Institut der Datensperrung soll über ein Recht auf Beschränkung der Datenverarbeitung in bestimmten Fällen erhalten bleiben.

In Art. 18 E-EU-DSGVO wird ein Recht auf Datenportabilität eingeführt. Betroffene sollen das Recht erhalten, ihre Daten aus einem automatisierten Datenverarbeitungssystem auf ein anderes System zu übertragen. Als Voraussetzung für die Ausübung dieses Rechts und um den Zugang Betroffener zu ihren Daten zu verbessern, soll die verantwortliche Stelle die Daten in einem strukturierten, gängigen elektronischen Format zur Verfügung stellen müssen.

2.5 Die Beteiligten – Begriffsbestimmung

Im Rahmen von Auskunftsersuchen wird eine Reihe von unterschiedlichen Konstellationen der Beteiligten behandelt. Die verwendeten Begrifflichkeiten sollen deshalb an dieser Stelle kurz beleuchtet werden.

2.5.1 Anfragende, Auskunftsersuchen, verantwortliche Stelle

Ein „klassisches" Auskunftsersuchen wird durch Anfragende (Synonym: Betroffene vgl. 2.1.2, Bürgerinnen und Bürger, Verbraucherinnen und Verbraucher, Nutzerinnen und Nutzer i. S. d. TMG, Teilnehmerinnen und Teilnehmer i. S. d. TKG) bei verantwortlichen Stellen (vgl. 2.1.2; Synonym: angefragte Stelle, (zumeist) Unternehmen) gestellt. Die verantwortliche Stelle sendet die Auskunft (Antwort auf das Auskunftsersuchen) an den Anfragenden.

2.5.2 Auskunftsersuchen mit Auskunftsportal

Bei einem Auskunftsersuchen mit Beteiligung eines Auskunftsportals (vgl. 2.5.3; Synonym: Portal) kann das Auskunftsersuchen verschiedene Wege nehmen:

- Anfragende erstellen das Auskunftsersuchen mit Hilfe des Auskunftsportals und senden es selbst an die verantwortliche Stelle.
- Anfragende erstellen das Auskunftsersuchen mit Hilfe des Auskunftsportals und das Portal übermittelt das Auskunftsersuchen an die verantwortliche Stelle.

Die verantwortliche Stelle sendet die Auskunft dann direkt an Anfragende. Eine Übermittlung der Auskunft über das Auskunftsportal ist nur mit entsprechenden Authentisierungskonzepten möglich, begegnet aber wegen der Konzentration verifizierter Daten bei einem Dritten grundsätzlichen datenschutzrechtlichen Bedenken (vgl. 3.3).

2.5.3 Auskunftsportal

Ein Auskunftsportals (Synonym: Portal) bietet über eine Webseite Hilfestellung zur Erstellung von Auskunftsersuchen an. Es ist selbst verantwortliche Stelle, wenn bei dem Betrieb personenbezoge-

ne Daten etwa der Anfragenden verwendet werden. Datenverwendungen durch das Auskunftsportal stehen als Synonym für Datenverwendungen durch den Betreiber des Portals. Der Betreiber des Portals ist Diensteanbieter nach dem TMG. Werden Dienste wie E-Mail-Versand angeboten, wird das Portal auch zum Telekommunikationsdiensteanbieter, das die Vorgaben des TKG zu beachten hat (vgl. 6).

3 Problemaufriss: Auskunftsersuchen durch Betroffene

Allgemeines zum Auskunftsrecht nach § 34 BDSG ist bereits unter 2.3.1 ausgeführt worden. Im Folgenden sollen insbesondere praktisch relevante Fragen dargestellt und Umsetzungshindernisse bei der Stellung eines Auskunftsersuchens durch Betroffene analysiert werden.

3.1 Anlässe für Auskunftsersuchen

Formal rechtlich müssen Betroffene gem. § 34 BDSG keinen Anlass i. S. e. berechtigten Interesses an der begehrten Auskunft vorweisen, um den Auskunftsanspruch durchsetzen zu können. In der Regel werden Verbraucherinnen und Verbraucher aber aufgrund eines konkreten Anlasses i. S. e. Ereignisses eine Auskunft nach § 34 BDSG verlangen. Mögliche Fallgruppen werden im Folgenden dargestellt und können beispielsweise bei der Kundeninformation und/oder der Benutzerführung (vgl. 6.1.2) Beachtung finden.

Allgemeine Anlässe für Auskunftsersuchen können Medienberichterstattungen etwa über Datenschutzskandale sein. Erfahrungsgemäß informieren sich Verbraucherinnen und Verbraucher in diesem Zusammenhang verstärkt über spezifische Rechte und haben aufgrund der konkretisierten Gefährdungslage eine erhöhte Motivation, Maßnahmen einzuleiten.

Konkreter Anlass, ein Auskunftsbegehren an ein Unternehmen zu richten, kann die Zusendung unaufgeforderter Werbung sein. Das Verhältnis der Verbraucherinnen und Verbraucher zu Werbung sowie Markt- und Meinungsforschung hat sich gewandelt.[18] Insbesondere unaufgefordert zugesendete Werbung wird zunehmend kritisch wahrgenommen. Betroffene hinterfragen verstärkt, wie die eigenen personenbezogenen Daten an den Absender gelangt sind und ob eine Erlaubnis für die Übermittlung und Nutzung besteht. Erfahrungsgemäß besteht ein besonderes Interesse der Betroffenen daran, die Kette der Datenübermittlungen aufzudecken, über die die Adressdaten zu dem Absender der Werbung gelangt sind. Der Gesetzgeber hat dieses Bedürfnis in der Novellierung des BDSG im Jahr 2009 berücksichtigt.[19]

Ein weiterer konkreter Anlass für Auskunftsersuchen können Kontaktaufnahmen anderer Art durch Auskunfteien oder vergleichbare Stellen sein. Durch die Datenschutzskandale der vergangenen Jahre sind Verbraucherinnen und Verbraucher sensibilisiert und hinterfragen entsprechende Kontaktaufnahmen, in denen beispielsweise um die Überprüfung und Aktualisierung zum Empfänger gespeicherter Daten gebeten wird. Grundsätzlich können Benachrichtigungen hinsichtlich der Übermittlung von Daten durch Stellen nach § 29 BDSG wie Auskunfteien, die geschäftsmäßig Datenerhebungen und -speicherungen zum Zweck der Übermittlung vornehmen, auch der Erfüllung gesetzlicher Benachrichtigungspflichten nach § 33 BDSG dienen. Es erscheint empfehlenswert, an einer prominenten und vertrauenswürdigen Stelle den Hintergrund und ggf. die gesetzliche Verpflichtung einer Kontaktaufnahme adressatenfreundlich darzustellen. So können Missverständnis-

[18] Bundestag-Drucksache 16/10529, S. 1, 10.10.2008.

[19] Bundestag-Drucksache 16/13657, S. 22, 01.07.2009.

se vermieden werden, die dem Image der verantwortlichen Stelle abträglich sein und zu arbeitsintensiven Rückfragen führen können.

Anlass für die Geltendmachung eines Auskunftsanspruchs kann zudem die Ablehnung eines Kredit- oder vergleichbaren Vertrags sein. Wenn für Betroffene diesbezüglich kein plausibler Grund ersichtlich ist, wird ein besonderes Informationsbedürfnis bestehen. Betroffene hinterfragen, welche Informationen die kreditgebende Stelle zu ihrer Person gespeichert hat, die möglicherweise in die Kreditentscheidung eingeflossen sind, und aus welchen Quellen diese erhoben wurden. In der Öffentlichkeit besteht ein vages Bewusstsein darüber, dass kreditgebende Stellen von dritten Stellen, so genannten Auskunfteien, Informationen zur Beurteilung der Kreditwürdigkeit ihrer Kunden erheben. Eine relativ bekannte Kreditauskunftei ist die Schufa Holding AG. Auch im Rahmen von Bestellungen beispielsweise bei Onlineshops werden Bonitätsprüfungen mit Hilfe von Auskunfteien vorgenommen. Auch hier ergeben sich Fragen, etwa welche Daten der Händler zum Betroffenen gespeichert hat und zu welchem Zweck dies geschieht, von welcher Stelle die Informationen stammen, und ob sie an dritte Stellen weitergegeben werden. Nicht zuletzt aufgrund der wirtschaftlichen Bedeutung dieser Datenverarbeitungszusammenhänge besteht ein zunehmendes Bedürfnis in der Öffentlichkeit, Klarheit über die Datenbestände, die Übermittlungen und deren Rechtmäßigkeit zu erhalten.

Betroffene werden auf Auskunfteien wie die Schufa zudem aufmerksam, wenn Datenverarbeitungsklauseln wie die sog. „Schufa-Klausel" unterschrieben werden. Derartige Klauseln kommen etwa in Girokonto-, Kredit- oder Telefonvertrag vor. Verbraucherinnen und Verbraucher hinterfragen zunehmend, was konkret hinter derartigen Klauseln steckt und welche Datenverarbeitungen darauf gestützt werden.

Fragen ergeben sich für Verbraucherinnen und Verbraucher zudem etwa, wenn sie mit ihrer EC-Karte gezahlt haben und einen Kassenzettel vorgelegt bekommen mit einer „Einwilligung gem. § 4a Bundesdatenschutzgesetz" oder einer ähnlichen Information, wonach ihre Daten durch ein weiteres Unternehmen verwendet werden. Es besteht ein Bedürfnis der Öffentlichkeit, Transparenz über die Datenverarbeitungsvorgänge EC-Transaktionen zu erhalten. Eine Auskunft soll hier klären, welche Daten von welchen Stellen zu dem Betroffenen gespeichert werden und für welche Zwecke dies erfolgt.

3.2 Informationsdefizit und Ausführungshindernisse

Unter Verbraucherinnen und Verbrauchern ist das Auskunftsrecht grundsätzlich bekannt.[20] Dennoch wird der Auskunftsanspruch laut einer Umfrage unter betrieblichen Datenschutzbeauftragten

[20] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Erhöhung des Datenschutzniveaus zugunsten der Verbraucher, Studie im Auftrag des Bundesministeriums für Verbraucherschutz, Ernährung und Landwirtschaft, 2006, S. 97. In einer Umfrage wussten 85,2 % der Befragten, dass das Unternehmen die Auskunft über die gespeicherten Daten nicht verweigern darf. https://www.datenschutzzentrum.de/verbraucherdatenschutz/uld-verbraucherdatenschutz-bmelv.pdf (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

selten geltend gemacht.[21] Ausführungshindernisse könnten aufgrund von Informationsdefiziten bestehen. Erfahrungsgemäß hat der Umgang mit Rechtsvorschriften auf Verbraucherinnen und Verbraucher in vielen Fällen eine „abschreckende Wirkung". Die konkrete Rechtsvorschrift, aus der sich der Auskunftsanspruch ergibt, wird ihnen nicht bekannt sein. Dementsprechend ist auch nicht der konkrete Umfang des Auskunftsanspruchs bekannt. Auskunftsbegehren können aber auch bereits an der Kenntnis der Anschrift einer bestimmten Stelle scheitern. Zudem könnte Verbraucherinnen und Verbrauchern ein Überblick zu bestimmten Unternehmen und Branchen wie beispielsweise der Adresshandelsbranche fehlen, zwischen und innerhalb derer Datenweitergaben zum Beispiel besonders wahrscheinlich sind.

Vorbehalte könnten auch bestehen, wenn durch das Auskunftsverlangen Kosten befürchtet werden oder andere Modalitäten eines Auskunftsersuchens unbekannt sind. So könnten beispielsweise Unsicherheiten bestehen, ob das Auskunftsersuchen einer bestimmten Form entsprechen muss, welche Angaben zur Identifizierung gemacht werden müssen und ob insbesondere eine Ausweiskopie zur Authentisierung vorgelegt werden muss (vgl. 2.3.2). Verbraucherinnen und Verbraucher dürften in der Regel Erfahrungswerte zum Ablauf des Auskunftsverfahrens fehlen. Es könnten beispielsweise Unsicherheiten bestehen, innerhalb welcher Frist eine Antwort erwartet werden und ob die angefragte Stelle eine Konkretisierung Auskunftsersuchens verlangen kann. Mangels detaillierten Einblicks in die Verfahren der datenverarbeitenden Stellen können solche Konkretisierungen von Verbraucherinnen und Verbrauchern in der Regel nicht geleistet werden.

3.3 Ausübung durch Dritte

Datenschutzrechte sind Persönlichkeitsrechte. Es stellt sich die Frage, ob Betroffenenrechte wie das Auskunftsrecht höchstpersönlich geltend gemacht werden müssen. In der Literatur wird einhellig angenommen, dass eine Vertretung möglich ist.[22] Vorausgesetzt wird allerdings, dass die verantwortliche Stelle die Vertretungsvollmacht überprüft.

Das Vertretenlassen kann entweder nur den Versand des Auskunftsbegehrens oder auch den Empfang der Auskunft umfassen. Vertreter im persönlichen Nahbereich weisen dabei keine strukturellen, über die allgemeinen Risiken hinausgehenden Probleme auf. Werden aber Dienstleister mit der Geltendmachung von Auskunftsrechten beauftragt, können persönlichkeitsrechtliche Risiken bestehen. Unseriöse Dienstleister stehen in dem Verdacht, zu beabsichtigen, über diesen „Service" primär verifizierte Daten für fremde Zwecke wie Datenhandel zu erheben. Generell ist eine zentrale Stellung eines Dritten bei der Abwicklung von Auskunftsersuchen datenschutzrechtlich kritisch zu bewerten (vgl. 5.5).

---

[21] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Erhöhung des Datenschutzniveaus zugunsten der Verbraucher, Studie im Auftrag des Bundesministeriums für Verbraucherschutz, Ernährung und Landwirtschaft, 2006 S. 107. https://www.datenschutzzentrum.de/verbraucherdatenschutz/uld-verbraucher-datenschutz-bmelv.pdf (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

[22] Dix in Simitis (Hrsg.), Kommentar zum BDSG, 7. Auflage 2011, § 34 Rn. 43; Gola / Schomerus, BDSG Kommentar, 11. Auflage 2012, § 34 Rn. 7; Däubler in Däubler / Klebe / Wedde / Weichert (Hrsg.), Bundesdatenschutzgesetz Kompaktkommentar, 3. Auflage 2010, § 34 Rn. 29; Meents in Taeger / Gabel, Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 1. Auflage 2010, § 34 BDSG Rn. 13.

Äußerst weitreichende Kenntnisse erhält ein Vertreter, der sogar mit dem Empfang der Auskunft beauftragt wird. Es ist fragwürdig, welchen Mehrwert dies für den Betroffenen bieten soll. Eine Überprüfung der gespeicherten Daten auf Richtigkeit kann nur der Betroffene selbst vornehmen. Jedenfalls ist die Erhebung und Speicherung der Auskunft bei einem Dienstleister nicht erforderlich. Seriöse Dienstleister werden daher eine eigene Kenntnisnahmemöglichkeit ausschließen.

3.4 Eskalationsmöglichkeiten

Die vorsätzliche oder fahrlässige Nichterteilung einer Auskunft stellt gem. § 43 Abs. 1 Nr. 8a BDSG eine Ordnungswidrigkeit dar. Ebenso handelt ordnungswidrig, wer Auskünfte nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt.

§ 34 BDSG sieht keine Frist vor, innerhalb derer Auskünfte zu erteilen sind. Das Auskunftsrecht dient vor allem der Kontrolle und ggf. der Geltendmachung von Berichtigungsansprüchen, um negative Konsequenzen beispielsweise durch die Verbreitung unrichtiger Daten abzuwenden. Daher muss eine Auskunft unverzüglich, das heißt ohne schuldhaftes Zögern[23], erfolgen.[24] Anfragende können der verantwortlichen Stelle zur Auskunftserteilung eine angemessene Frist setzen, die organisatorische Abläufe der verantwortlichen Stellen beachtet. Eine Frist von drei Wochen kann in der Regel als angemessen angesehen werden. Erfolgt auch auf eine Erinnerung keine Auskunft, kann die zuständige Aufsichtsbehörde für den Datenschutz informiert werden.

§ 34 Abs. 2 S. 1 Nr. 3, Abs. 4 S. 1 Nr. 4 BDSG fordert ausdrücklich eine verständliche Auskunft hinsichtlich des Zustandekommens von Wahrscheinlichkeitswerten, das heißt zu Scorewertberechnungen. Ausgehend vom Sinn und Zweck des Auskunftsanspruchs im Allgemeinen, die informationelle Selbstbestimmung der Betroffenen zu gewährleisten, muss die Verständlichkeit aber ein generelles Kriterium für die Richtig- bzw. Vollständigkeit einer Auskunft sein. Insbesondere erkennt aber auch Art. 12 lit. a EG-DSRL Verständlichkeit als ein Wesensmerkmal des Auskunftsanspruchs im Allgemeinen (vgl. 4.1.3).

Die Zuständigkeit der Datenschutzaufsichtsbehörden der Länder richtet sich grundsätzlich nach dem Sitz der verantwortlichen Stelle. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) nimmt die Aufsicht über Bundesbehörden sowie über Post- und Telekommunikationsunternehmen wahr. Die Aufsichtsbehörden kontrollieren gem. § 38 BDSG die Ausführung der Datenschutzvorschriften durch nicht-öffentliche Stellen. Dafür können die Behörden verlangen, von den verantwortlichen Stellen unverzüglich die für die Erfüllung ihrer Aufgabe erforderlichen Auskünfte zu erhalten. Während der Betriebs- und Geschäftszeiten können Prüfungen in Geschäftsräumen der verantwortlichen Stelle vorgenommen werden. Es darf Einsicht genommen werden in Datenverarbeitungsprogramme und gespeicherte personenbezogene Daten. Bei der Feststellung von Verstößen gegen Datenschutzvorschriften können Maßnahmen zur Beseitigung angeordnet werden. Bei schwerwiegenden Verstößen, die nicht beseitigt werden, kann die Erhe-

[23] § 121 Abs. 1 S. 1 BGB.

[24] Däubler in Däubler / Klebe / Wedde / Weichert (Hrsg.), Bundesdatenschutzgesetz Kompaktkommentar, 3. Auflage 2010, § 34 Rn. 25.

bung, Verarbeitung und Nutzung personenbezogener Daten oder der Einsatz von Verfahren untersagt werden.

Medienorgane wie Presse und Rundfunk sind hinsichtlich der journalistisch-redaktionellen Tätigkeit vom Anwendungsbereich des BDSG ausgenommen. Damit sind sie auch von den Kontrollbefugnissen der Aufsichtsbehörden, der Landes- und des Bundesdatenschutzbeauftragten ausgenommen. Die öffentlich-rechtlichen Sendeanstalten haben Rundfunkdatenschutzbeauftragte bestellt. Die Aufsicht über öffentliche Stellen auf Landesebene nehmen die Landesbeauftragten für Datenschutz wahr. Für die Kontrolle der Verarbeitung personenbezogener Daten durch kirchliche Stellen sind die Datenschutzbeauftragten der Kirchen zuständig.

4 Auskunftserteilung durch Unternehmen

An Auskünfte nach § 34 BDSG werden bestimmte gesetzliche Anforderungen gestellt. Zudem nehmen auch die Betroffenen den Umgang der verantwortlichen Stelle mit Auskunftsersuchen als Teil der Kundenkommunikation und imagebildende Maßnahme wahr. Den Erwartungen der Betroffenen sowie den gesetzlichen Qualitätsanforderungen zuverlässig und effizient gerecht zu werden, kann sich allerdings aus verschiedenen Gründen als Herausforderung darstellen. So können unklare Formulierungen in den Auskunftsersuchen einen erhöhten Arbeitsaufwand erzeugen. Jedes Auskunftsersuchen muss in diesem Fall einzeln einer Interpretation unterzogen werden. Ggf. müssen Rückfragen an den Auskunftssuchenden gerichtet werden. Nicht zuletzt unkonkrete oder falsche Adressierungen können Verzögerungen oder zusätzliche Arbeitsabläufe verursachen. Die Adressaten der Auskunftsersuchen, wie z. B. Unternehmen, müssen aufgrund der andernfalls drohenden Sanktionen ein hohes Maß an Sorgfalt bei der Erteilung von Auskünften anwenden. Für die Auskunfts- und Kommunikationsstruktur der Organisation sollte ein generelles Konzept bestehen. Die gesetzlichen Anforderungen, rechtliche Risiken bei der Nichteinhaltung sowie Möglichkeiten, die Einhaltung dieser Anforderungen strukturell zu gewährleisten, sollen im Folgenden dargestellt werden.

4.1 Qualität der Auskunft

§ 34 BDSG selbst enthält keine abschließende Vorgabe formeller und materieller Anforderungen an die Erteilung von Auskünften. In formeller Hinsicht wird in § 34 Abs. 6, Abs. 8 BDSG lediglich vorgegeben, dass eine Auskunft auf Verlangen grundsätzlich in Textform und grundsätzlich unentgeltlich zu erteilen ist (vgl. 2.3.1). Ist die Auskunft nicht unentgeltlich, muss darauf hingewiesen werden, dass die Möglichkeit besteht, sich persönlich Kenntnis über die betreffenden Daten zu verschaffen. In materieller Hinsicht sehen § 34 Abs. 1, 1a, 2, 3, 4 BDSG Vorgaben zum Umfang des Auskunftsanspruchs vor, der jeweils vom Betroffenen geltend gemacht werden muss. § 34 Abs. 7 BDSG schränkt die Pflicht zur Auskunftserteilung für den Fall ein, dass der Betroffene nach § 33 Abs. 2 S. 1 Nr. 2, 3, 5, 6, 7 BDSG auch nicht zu benachrichtigen wäre. Dies kann insbesondere der Fall sein, wenn die Auskunft die rechtlichen Interessen eines Dritten beeinträchtigen würde. § 34 Abs. 1 S. 4 und Abs. 3 S. 3 beschränken den Auskunftsanspruch zudem jeweils für den Fall, dass bei Auskunft über die Herkunft und die Empfänger das Interesse an der Wahrung des Geschäftsgeheimnisses der verantwortlichen Stelle gegenüber dem Informationsinteresse des Betroffenen überwiegt. Insofern ist eine Abwägung im Einzelfall vorzunehmen. Ausweislich des Wortlauts sind die Kategorien von Empfängern nicht von der Ausnahme erfasst, sondern müssen beauskunftet werden. Im Übrigen sehen § 34 Abs. 1a, 2 und 4 BDSG keine Ausnahmen unter Berücksichtigung der Geschäftsgeheimnisse der verantwortlichen Stelle vor. Die Rechtsprechung[25] hat hieraus geschlossen, dass für diese Auskunftsansprüche insbesondere zu den Score- bzw. Wahrscheinlichkeitswerten etwa entgegenstehende Geschäftsgeheimnisse keine Berücksichtigung finden sollen.

[25] LG Berlin, Urteil vom 01.11.2011, Az. 6 O 479/10.

Aus § 43 Abs. 2 Nr. 1 BDSG ergibt sich die Vorgabe, dass personenbezogene Daten nicht unbefugt übermittelt werden dürfen. Insofern dürfen Auskünfte nicht an unberechtigte Dritte übermittelt werden. Um dieser Vorgabe gerecht zu werden, müssen adäquate Authentisierungsmaßnahmen angewandt werden (vgl. 2.3.2).

Vorgaben an die Auskunftserteilung ergeben sich auch aus § 43 Abs. 1 Nr. 8a-8c BDSG. Hiernach ist es insbesondere bußgeldbewehrt, wenn eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt wird.

4.1.1 Vollständig

Die Voraussetzung der Vollständigkeit ist nur erfüllt, wenn das Auskunftsersuchen des Betroffenen umfassend beantwortet ist. Hat der Betroffene Auskunft über die zu seiner Person gespeicherten Daten verlangt, müssen grundsätzlich alle entsprechenden Informationen erteilt werden. Der Auskunftsanspruch des § 34 BDSG erfasst gem. § 27 Abs. 1 S. 1 BDSG allerdings nur Daten, die in oder aus nicht automatisierten Dateien gem. § 3 Abs. 2 S. 2 BDSG oder unter Einsatz von Datenverarbeitungsanlagen gem. § 3 Abs. 2 S. 1 BDSG verarbeitet werden. Daten zur Person des Betroffenen in einer Papierakte, die nicht gleichartig aufgebaut und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann, unterfallen somit nicht dem Auskunftsanspruch. Erfasst sind nur personenbezogene Daten (vgl. 2.1.1). Ausnahmen bestehen nach § 34 Abs. 3 BDSG (vgl. 2.3.1) für Stellen, die geschäftsmäßig zum Zweck der Übermittlung Daten verarbeiten, wie Adresshändler und Auskunfteien.

Um die Anforderung der Vollständigkeit zu erfüllen, ist bei der Auslegung der Vorgaben des § 34 BDSG der Sinn und Zweck der Vorschrift zu berücksichtigen. Der besteht u. a. auch darin, Betroffene in die Lage zu versetzen, das Recht auf informationelle Selbstbestimmung ebenfalls gegenüber weiteren Datenempfängern wahrnehmen zu können. Nach dem Wortlaut des § 34 Abs. 1 S. 1 Nr. 2 BDSG muss Auskunft erteilt werden über „Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben *werden*". Nach der Rechtsprechung des EuGH[26] und dem Gesetzeswortlaut[27] muss Auskunft darüber erteilt werden, an welche Stellen Daten weitergegeben wurden sowie weitergegeben werden können. Der Auskunftsanspruch hinsichtlich der Empfänger oder Kategorien von Empfängern ist nicht auf die gespeicherten Angaben beschränkt, denn im Gegensatz zu § 34 Abs. 1 S. 1 Nr. 1 BDSG ist eine solche Einschränkung nicht normiert. § 34 Abs. 1 S. 1 Nr. 2 BDSG impliziert die Vorgabe für die verantwortlichen Stellen, Angaben über die Empfänger sowie die Kategorien von Empfängern zu erfassen und zu speichern, um sie beauskunften zu können (vgl. 2.3.1).[28]

---

[26] So auch Urteil des EuGH vom 07.05.2009, Az. C-553/07, Rn. 54, „Hierzu ist festzustellen, dass das betreffende [Auskunfts-]Recht [hinsichtlich Empfängern und Kategorien von Empfängern], um die praktische Wirksamkeit […] zu gewährleisten, zwingend für die Vergangenheit gelten muss. Denn andernfalls wäre die betroffene Person weder in der Lage, wirksam ihr Recht auf Veranlassung der Berichtigung, Löschung oder Sperrung von Daten wahrzunehmen, die ihrer Ansicht nach unbefugt verarbeitet wurden oder falsch sind, noch, einen gerichtlichen Rechtsbehelf einzulegen und Schadensersatz zu erlangen."

[27] Vgl. § 4e Nr. 6 BDSG.

[28] Dix in Simitis (Hrsg.), Kommentar zum BDSG, 7. Auflage 2011, § 34 Rn. 23.

Vollständigkeit ist zudem nur gegeben, wenn beispielsweise auch Bewertungen und Ableitungen, die auf der Grundlage von „Rohdaten" zu der Person getroffen werden, beauskunftet werden (vgl. 4.1.3). Nur anhand dieser Auskunft können Betroffene den Informationsstand der speichernden Stelle richtig und umfassend einschätzen, was das Recht auf informationelle Selbstbestimmung garantiert. Denn dieses Recht umfasst die Möglichkeit des Einzelnen zu erfahren, wer was wann und bei welcher Gelegenheit über ihn weiß.[29] Es geht demnach um ein informationelles Kräftegleichgewicht. Die Kenntnis von Bewertungen ist eine wesentliche Voraussetzung dafür, das informationelle Kräftegleichgewicht aufrecht zu erhalten, da die Aggregation, Bewertung und Einordnung von Daten unter den Umständen einer zunehmenden „Datenflut" und unbegrenzten technischen Speichermöglichkeiten entsprechend an Bedeutung zunimmt.

Eine Herausforderung bei der Gewährleistung der Vollständigkeit kann darin bestehen, alle Speicherorte und Datenverarbeitungsverfahren zu identifizieren, in denen Daten zu dem Anfragenden vorhanden sind. Dies kann nur bewältigt werden, wenn eine zuverlässige Dokumentation zu den Datenverarbeitungsverfahren (vgl. 6.2.3.2) sowie ein Konzept für die Auskunftserteilung existiert.

4.1.2 Richtig

Eine Auskunft wird als richtig angesehen, wenn sie den Tatsachen entspricht. Das heißt, dass eine Auskunft insbesondere genau die Daten wieder zu geben hat, die zu dem Anfragenden gespeichert werden. Werden abgeänderte beispielsweise um Bewertungen (vgl. 4.1.1) reduzierte Angaben gemacht, handelt es sich um unrichtige Auskünfte.

4.1.3 Verständlich

Die Verständlichkeit der Auskunft über die gespeicherten Daten und deren Herkunft ist gem. Art. 12 lit. a EG-DSRL ein Wesensmerkmal des Auskunftsanspruchs. Diese Voraussetzung findet sich sowohl in den Kriterien „vollständige" als auch „richtige" Auskunft wieder (vgl. 4.1.1 und 4.1.2). Generell fordert die Maßgabe der Verständlichkeit allgemeinverständliche bzw. ggf. adressatengerechte Formulierungen und Darstellungen. Je nach Aggregierungsform der Daten müssen zudem Hilfsmittel für den Betroffenen angeboten bzw. eingesetzt werden, damit dieser die beauskunfteten Informationen verstehen kann. Verschlüsselte Daten müssen somit jedenfalls entschlüsselt beauskunftet werden.[30] Zudem ist die Voraussetzung Verständlichkeit nur erfüllt, wenn erklärungsbedürftige Zusammenhänge erläutert werden. Ergibt sich die Bedeutung einer Information z. B. durch die Einordnung in eine Kategorie, ist dies darzustellen. Werden zu dem Betroffenen etwa die Einsätze der Kundenkarte gespeichert und wird aus der Häufigkeit >20 pro Jahr abgeleitet, dass es sich um einen „aktiven Kunden" handelt, ist dieser Rückschluss mitzuteilen. Nur unter dieser Voraussetzung werden „Rohdaten", auf deren Grundlage Ableitungen vorgenommen werden, verständlich beauskunftet.

---

[29] Urteil des Bundesverfassungsgerichts vom 15.12.1983 (Volkszählungsurteil), Rn. 148.

[30] Däubler in Däubler / Klebe / Wedde / Weichert (Hrsg.), Bundesdatenschutzgesetz Kompaktkommentar, 3. Auflage 2010, § 34 Rn. 31.

4.1.4 Rechtzeitig

Der unverzüglichen und reibungslosen Bearbeitung von Auskunftsersuchen kommt eine hohe Bedeutung zu. Denn durch die Auskunft können unrichtig gespeicherte Daten sowie andere Beeinträchtigungen der Persönlichkeitsrechte der Betroffenen erkannt und beseitigt werden. Durch eine Verzögerung der Auskunft würde auch die Beeinträchtigung der Persönlichkeitsrechte in unzumutbarer Weise weiter andauern. Ggf. verstärkt sich die Beeinträchtigung sogar, beispielsweise durch die zwischenzeitliche Verbreitung[31] unrichtiger Daten. Daher sind Auskünfte unverzüglich, d. h. gem. § 121 Abs. 1 S. 1 BGB ohne schuldhaftes Zögern, zu erteilen.[32] Nach Art. 12 E-EU-DSGVO könnte zukünftig grundsätzlich eine Auskunftsfrist von einem Monat gelten. Diese Frist kann sicherlich auch heute schon als maximale Orientierungsgröße gelten. Gem. Art. 12 lit. a EG-DSRL, der aktuell bei der Auslegung des § 34 BDSG zu beachten ist, dürfen keine unzumutbaren Verzögerungen eintreten. Dies kann nur erfüllt werden, wenn eine zuverlässige Dokumentation zu den Datenverarbeitungsverfahren (vgl. 6.2.3.2) sowie ein Konzept für die Erteilung von Auskünften existiert. Andernfalls ist der Aufgabe zeitaufwendig mit jeder Anfrage neu zu erfassen (vgl. 4.2).

4.1.5 Qualitätskontrolle

Eine vollständige, richtige, verständliche, rechtzeitige Auskunft zu erteilen, ist nur unter Beachtung insbesondere der dargestellten Anforderungen möglich. In Anbetracht zunehmend arbeitsteiliger Arbeitsabläufe und sich schnell ändernder Organisationsstrukturen ist der Kontrolle des Auskunftsergebnisses ein hoher Stellenwert beizumessen. Insbesondere wenn Erkenntnisse aus verschiedenen Organisationseinheiten zusammengeführt werden, ist eine Kontrolle des Ergebnisses von herausragender Bedeutung. Der Entwurf einer Auskunft muss insbesondere auf Vollständigkeit, Richtigkeit und Verständlichkeit überprüft werden. Dies muss idealerweise durch einen unabhängigen Funktionsträger in der Organisation erfolgen. Dieser muss über entsprechende Hilfsmittel wie Verfahrensdokumentationen und ausreichende Zugriffsrechte auf entsprechende Anwendungen verfügen, um die Kontrolle vornehmen zu können.

Unabhängig von konkreten Auskunftserteilungen muss auf konzeptioneller Ebene regelmäßig überprüft werden, ob die Qualitätskriterien fortlaufend erfüllt werden. So muss beispielsweise regelmäßig kontrolliert werden, ob die Vollständigkeit und Verständlichkeit beispielsweise verwendeter Mustertexte gegeben ist. Dabei sind insbesondere Änderungen in der Rechtslage und der Datenverarbeitungsverfahren der verantwortlichen Stelle zu beachten. Auch häufige Rückfragen und Beschwerden der Betroffenen können hier Hinweise geben und müssen entsprechend erfasst und dem Qualitätssicherungsverfahren zugeführt werden. Diese Maßgabe muss etwa in einem übergeordneten Beschwerdemanagementverfahren implementiert werden.

---

[31] Zur ohnehin bestehenden „besonderen Gefährdung persönlichkeitsrechtlicher Interessen, die mit der Verbreitung [personenbezogener Informationen] verbunden“ sind: BGH NJW 16.09.1966, S. 2353, 2354.

[32] Däubler in Däubler / Klebe / Wedde / Weichert (Hrsg.), Bundesdatenschutzgesetz Kompaktkommentar, 3. Auflage 2010, § 34 Rn. 25.

4.2 Kosten und Effizienz

Auskunftsersuchen verursachen bei der verantwortlichen Stelle Aufwand und Kosten. Der Gesetzgeber hat insofern eine Interessenabwägung zu Gunsten der Wahrnehmung der informationellen Selbstbestimmung des Einzelnen getroffen. Die gesetzlichen Pflichten müssen aufgrund ihrer Bedeutung mit großer Sorgfalt erfüllt werden. Fehlen beispielsweise in einem Auskunftsschreiben Angaben, ist es als unvollständig zu bewerten. Das Gesetz sieht kein mehrstufiges Verfahren vor. Es ist demnach nicht zulässig, Auskünfte sukzessive, beispielsweise erst auf Rückfrage zu erteilen. Vielmehr müssen unmittelbar alle Qualitätskriterien erfüllt sein. Dementsprechend ist die Auskunft auch rechtzeitig zu erteilen. Selbst wenn der Anfragende keine Frist setzt, wird nur ein Bearbeitungszeitraum von höchstens einem Monat als zumutbar anzusehen sein, wobei auch Postlaufzeiten zu beachten sind. Insofern muss in verhältnismäßig kurzer Zeit eine Aufgabe erfüllt werden, die verschiedene Organisationseinheiten betreffen kann und bestimmten Qualitätskriterien (vgl. 4.1) zu entsprechen hat.

Effizienzgesichtspunkte sind bei der Wahl der genutzten Verfahrenswege nicht allein ausschlaggebend. Vielmehr müssen diese zulässig sein, also insbesondere die schutzwürdigen Interessen der Betroffenen berücksichtigen. So mag zwar der Versand von Auskünften per Post einen hohen Kostenanteil darstellen. Dies allein rechtfertigt allerdings nicht den Versand etwa im kostengünstigeren E-Mail-Verfahren. Im unverschlüsselten E-Mail-Verfahren besteht kein adäquater Schutz gegen die Kenntnisnahme der Inhalte durch unberechtigte Dritte (zum Verbot der Übermittlung an unberechtigte Dritte vgl. 2.3.2). Zudem ist auch die Absicherung der Zustellung nur an den berechtigten Empfänger nicht wie im postalischen Verfahren möglich.

Die Effizienz der Aufgabenerfüllung kann gesteigert werden, wenn komplexe und wiederkehrende Arbeitsschritte als Prozesse definiert werden. Es ist betriebswirtschaftlich nicht zu vertreten, für verschiedene Auskunftsersuchen jeweils Arbeitszeit und -aufwand zu verwenden, um die Grundlagen der Auskunftserteilung jeweils neu zu erarbeiten. Vor allem besteht in diesem Fall ein hohes Risiko, dass Aspekte zur Erfüllung der Qualitätskriterien außer Acht gelassen werden.

4.3 Risiken und Rechtsfolgen

Dem Auskunftsrecht wird eine hohe Bedeutung beigemessen. Dies kommt u. a. durch die Unabdingbarkeit gem. § 6 BDSG zum Ausdruck, aber auch durch die Sanktionsbewehrtheit gem. § 43 Abs. 1 Nr. 8a-8c BDSG. Werden die Qualitätskriterien an die Auskunft nach § 34 BDSG (vgl. 4.1) nicht erfüllt, drohen Bußgelder bis zu 50.000 Euro.

Werden personenbezogene Daten unbefugt verarbeitet, das heißt etwa an einen unberechtigten Dritten übermittelt, stellt dies einen Bußgeldtatbestand gem. § 43 Abs. 2 Nr. 1 BDSG dar. Werden also beispielsweise Anfragende nicht ausreichend identifiziert und Auskünfte an Unberechtigte erteilt oder kommen Auskünfte auf einem unsicheren Übertragungsweg abhanden, drohen Bußgelder bis zu 300.000 Euro.

Zur Gewährleistung der Einhaltung der Datenschutzvorschriften können Datenschutzaufsichtsbehörden gem. § 38 Abs. 5 BDSG Anordnungen zur Beseitigung festgestellter Verstöße bei der Erhe-

bung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel nach § 9 BDSG i. V. m. Anlage zum BDSG treffen. Ein solcher Mangel läge etwa vor, wenn Verfahren zur elektronischen Übertragung personenbezogener Daten ohne Verschlüsselungstechnologie nach dem Stand der Technik eingesetzt würden.

Stellt die Aufsichtsbehörde fest, dass der betriebliche Datenschutzbeauftragte etwa die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt, kann sie dessen Abberufung verlangen. Treten systematische Fehler bei der Auskunftserteilung auf oder fehlen in komplexen Organisationen grundlegende Arbeitsanweisungen und Verfahrensvorgaben zur Erfüllung des Auskunftsanspruchs, können Zweifel an der Eignung und Fachkunde des betrieblichen Datenschutzbeauftragten entstehen.

4.4 Öffentlichkeitswirkung

Die Sensibilität für Datenschutzfragen hat in der Öffentlichkeit zugenommen. Verschiedene Datenschutzskandale haben die Medienwirksamkeit der Thematik erhöht. Datenverarbeitungsvorgängen wie Auskunftsprozesse werden als Aushängeschilder des Verhältnisses einer Organisation zur Einhaltung der Datenschutzvorschriften wahrgenommen. Defizite in diesem Bereich werden hingegen als Zeichen mangelnder Wertschätzung gegenüber den Betroffenen eingeordnet. Dies kann Auswirkungen auf das gesamte Renommee einer Organisation haben, das es sich möglicherweise mit aufwendigen Imagekampagnen aufgebaut hat.

Datenschutz und der Umgang mit den Betroffenenrechten wie Auskunftsersuchen ist ein Aspekt der Außendarstellung. Der Bereich sollte daher nicht als auferlegte Pflichtaufgabe des Gesetzgebers verstanden, sondern als Wettbewerbsvorteil genutzt werden. Es bietet die Möglichkeit, sich von Mitbewerbern durch ein vorbildliches Datenschutzkonzept abzugrenzen.

4.5 Optimierung

Den unter 4.3 und 4.4 beschriebenen Risiken kann durch organisatorische Maßnahmen entgegengewirkt werden. § 9 BDSG sowie die Anlage zu § 9 BDSG geben einen Mindeststandard vor (vgl. 6.2.3). Eine Organisation sollte einen auf die eigene Struktur zugeschnittenen Prozess aufsetzen, der die Grundvoraussetzungen für die Einhaltung der Datenschutzvorschriften insbesondere in einer arbeitsteiligen Organisation bietet.

5 Lösungsansatz: Auskunftsportal

5.1 Etablierung von Auskunftsprozessen

Für Unternehmen sind Gewinn bzw. Rentabilität zentrale, aber nicht die alleinigen Ziele.[33] Für viele Unternehmen ist dabei die Definition von Prozessen einen zentrales Element und der Ansatzpunkt für weitere Optimierung. Unter dem Aspekt der Wirtschaftlichkeit besteht jedoch auch die Option der Nichtregelung eines Prozesses. Die Zuständigkeit ergibt sich dann aus der Zuordnung der Verantwortlichkeit. Dies ist jedoch nur eine Option für selten vorkommende Geschäftsvorfälle, für die keine gesetzlichen Vorschriften existieren.[34] Die Nichtregulierung von einzelnen Prozessen ist jedoch nur wirtschaftlich, wenn die Kosten für das Prozessmanagement in diesem Fall höher sind als die zusätzlichen Kosten, die durch Reibungsverluste entstehen. Die Nichtregelung von Geschäftsvorfällen birgt zudem die Gefahr, dass Geschäftsvorfälle mit unterschiedlichen Qualitätsniveaus bearbeitet werden. Hier gilt es, die unterschiedlichen Zielsetzungen wie beispielweise Gewinn- und Qualitätsstreben durch die Unternehmensleitung gegeneinander abzuwägen.

Im Bereich von Auskunftsprozessen, die auf gesetzlichen Datenschutzvorgaben aufsetzen, sind die oben dargestellten Erwägungen zu ergänzen, da neben rein monetären Zielen und Qualitätsbestrebungen weitere Variablen zu berücksichtigen sind. Unternehmen[35], die keine oder falsche Auskünfte erteilen, drohen Bußgelder oder Anordnungen der zuständigen Datenschutzaufsichtsbehörden (vgl. 4.3) sowie Imageschäden (vgl. 4.4). Defizite bei der Auskunftserteilung führen erfahrungsgemäß zu Zweifeln bei den Betroffenen und in der öffentlichen Wahrnehmung, ob das Unternehmen generell in Datenschutzbelangen optimal aufgestellt ist und beispielweise mit Kundendaten sorgfältig umgeht.

Zusammenfassend lässt sich festhalten, dass es für Unternehmen empfehlenswert ist, Datenschutzprozesse, also auch die Auskunftsprozesse, unabhängig von übergeordneten Unternehmenszielen zuverlässig zu regeln. Dies bietet die Chance, diese Vorgänge wie etwa Auskunftsersuchen mit gleichbleibend hoher oder steigender Qualität zu bearbeiten. Verbraucherinnen und Verbraucher werden diese Entwicklung positiv bewerten, denn sie sind zunehmend gut über ihre Aus-

[33] Gablers Wirtschaftslexikon, Unternehmensziele.
http://wirtschaftslexikon.gabler.de/Definition/unternehmungsziele.html (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

[34] So sind etwa Notfallpläne wie beispielweise Evakuierungspläne gesetzlich vorgeschrieben.

[35] In diesem Fall verantwortliche Stelle, vgl. 2.1.2.

kunftsrechte informiert[36] und üben diese aus[37]. Etablierte Prozesse, insbesondere mit einem hohen Reifegrad, sind zudem regelmäßig auch unter Kostengesichtspunkten positiv zu bewerten.[38]

5.2 Grundüberlegungen zu Datenschutzprozessen

Ausgereifte Prozesse helfen verantwortlichen Stellen, die spezifischen Aufgaben der Organisation zuverlässig und effizient zu bewältigen. Selbst Standardaufgaben, wie Anträge auf Auskunft, Löschung, Sperrung oder Korrektur personenbezogener Daten (vgl. 2.2), können einen gewissen Komplexitätsgrad bergen, je nachdem wie spezifisch bzw. unspezifisch das Ersuchen durch den Anfragenden gestellt wird und wie komplex die Datenverarbeitungsverfahren der verantwortlichen Stelle sind. Macht ein Betroffener unter Nennung seines Namens und seiner Adresse sein Auskunftsrecht gegenüber einem Unternehmen geltend, so muss es sich nicht zwingend um einen Kunden handeln. Es könnte sich beispielweise auch um einen Mitarbeiter, ehemaligen Mitarbeiter, Mitarbeiter eines Zulieferers oder Dienstleisters, Bewerber oder Teilnehmer eines Gewinnspiels handeln. Dementsprechend können Daten zu seiner Person in unterschiedlichen Verfahren verwendet werden. Dies zeigt, wie wichtig das Führen von Verfahrensverzeichnissen (vgl. 6.2.3.2) ist. Nur so können die vielfältigen Formen der Verwendung personenbezogener Daten in einem Unternehmen entsprechend abgebildet und für die Etablierung der Datenschutzprozesse genutzt werden. Außerdem sollte ein betrieblicher Datenschutzbeauftragter (vgl. 2.1.9) bestellt und bei relevanten Entscheidungen standardmäßig einbezogen werden (vgl. 6.2.3.1). Der Grundstein für ein umfassendes Datenschutzmanagement ist so gelegt (vgl. 6.2.3.7). Ein ausgereifter Datenschutzmanagementprozess stellt sicher, dass alle Belange des Datenschutzes innerhalb einer verantwortlichen Stelle organisiert und dokumentiert sowie einer ständigen Überprüfung und Anpassung unterzogen werden. Dies stellt aus Sicht des Datenschutzes eine Möglichkeit dar, die gesetzlichen Anforderungen des Datenschutzes in die Unternehmensstruktur einzubinden.

Ein Auskunftsportal kann dabei unterstützen, die Prozesskette bereits bei dem Anfragenden beginnen zu lassen. Insbesondere kann es ihm die Möglichkeit bieten, die relevanten Identifikationsdaten strukturiert zu erfassen und mit Hilfe von Mustertexten eindeutig formulierte Auskunftsersuchen zu erstellen. So können Auskunftsersuchen beim Eintreffen im Unternehmen unproblematischer in die unternehmensinternen Prozesse integriert werden. Ohne diese Unterstützung müssen eingehende Auskunftsersuchen individuell erfasst und deren Inhalt klassifiziert werden. So ist etwa zu bestimmen, ob es sich beispielsweise um ein Auskunftsersuchen, eine Frage nach dem öffentlichen Verfahrensverzeichnis oder die Geltendmachung anderer Verbraucherrechte handelt. Anfragende verwenden nicht immer die korrekten rechtlichen Begriffe und eindeutige Formulierungen.

---

[36] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Erhöhung des Datenschutzniveaus zugunsten der Verbraucher, Studie im Auftrag des Bundesministeriums für Verbraucherschutz, Ernährung und Landwirtschaft, 2006, S. 97. https://www.datenschutzzentrum.de/verbraucherdatenschutz/uld-verbraucher-datenschutz-bmelv.pdf (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

[37] Beispielweise: Pressemitteilung zum Anstieg der Selbstauskünfte bei der Schufa nach der Änderung des BDSG, 19.05.2010. http://www.schufa.de/de/private/presse/aktuellepressemitteilungen/2010/100519.jsp (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

[38] Meints, Datenschutz durch Prozesse, DuD 2007, S. 95.

Zudem werden individuelle Formate für die Auskunftsersuchen verwendet, die eine standardisierte Erfassung behindern. Eingehende Anfragen werden deshalb regelmäßig manuell und damit kostenintensiv von der verantwortlichen Stelle dem Inhalt nach bewertet.

Die Prozessorientierung verantwortlicher Stellen darf natürlich nicht dazu führen, dass nur noch standardisierte und – etwa durch ein Portal – vorformulierte Auskunftsersuchen akzeptiert werden. Eine solche Formvorgabe für Auskunftsersuchen wäre nicht nur gesetzlich nicht gerechtfertigt, sondern widerspräche sogar der Intention des Auskunftsanspruchs nach § 34 BDSG (vgl. 2.3.1). Sollte sich die Bearbeitungszeit von Auskunftsersuchen durch die Nutzung eines Auskunftsportal allerdings verkürzen, so wäre dies im Interesse des effektiven Schutzes der Persönlichkeitsrechte der Betroffenen positiv zu bewerten (vgl. 4.1.4).

5.3 Steigerung des Datenschutzniveaus

Die vorangegangen Abschnitte haben einige Vorteile eines Auskunftsportals für verantwortliche Stellen beschrieben. Zudem kann eine Auskunftsportal als eine zentrale Anlaufstelle für Verbraucherinnen und Verbraucher einen Beitrag zur Erhöhung des Datenschutzniveaus leisten. So kann an einer solchen zentralen Stelle etwa über Datenschutzrechte informiert und beispielsweise hinsichtlich spezifischer Problemfelder sensibilisiert werden. Zudem besteht die Möglichkeit, ggf. angebundene verantwortliche Stellen wie Unternehmen über ihre rechtlichen Pflichten aufzuklären. Beide Parteien können so im Idealfall mit dem gleichen Wissensstand auf Augenhöhe miteinander kommunizieren. Ein solches Portal nimmt eine verantwortungsvolle Rolle bei der Wahrnehmung der Interessen zwischen Betroffenen und verantwortlichen Stellen ein.

Beim Portalbetreiber können im Rahmen dieser Tätigkeit eine Reihe von Daten der Nutzerinnen und Nutzer des Portals anfallen. Das Portal sollte somit die Voraussetzungen bieten, das Vertrauen beider Parteien, insbesondere der Verbraucherinnen und Verbraucher, zu erhalten. Diesen Anspruch kann ein Auskunftsportal nur erfüllen, wenn es insbesondere den Grundsatz der Transparenz in vorbildlicher Weise erfüllt. Transparent kommuniziert werden sollte auch, in welcher Gesellschaftsform das Portal betrieben wird, welche Gesellschafter das Portal betreiben und wie bzw. durch welche Leistungen das Auskunftsportal finanziert wird. Es muss deutlich werden, welche Interessen Gesellschaftsform, Gesellschafter und Finanzierungsmodell verfolgen, und ob ein Auskunftsportal etwa einseitig beispielsweise unternehmerischen Interessen dient.

Ein zentrales Auskunftsportal kann auch der Unterstützung der Tätigkeit der Aufsichtsbehörden sowie von Organisationen, die Verbraucherrechte vertreten, dienen. So könnten etwa an prominenter Stelle Forderungen und Ansichten zu generellen und tagesaktuellen daten- und verbraucherschutzrechtlichen Fragen kommuniziert werden.

Sollte sich ein Auskunftsportal etablieren und sowohl von verantwortlichen Stellen als auch von Verbraucherinnen und Verbrauchern angenommen werden, so werden an dieser Stelle Standards hinsichtlich der Erteilung von Auskünften gesetzt. Diese können auch auf die Auslegung bestehender gesetzlicher Regelungen Auswirkungen haben.

5.4 Ökonomische Gesichtspunkte zum Medienbruch

Eine volldigitalisierte prozessuale Abwicklung der Auskunft, von der Stellung und dem Empfang des Auskunftsersuchens über die Bearbeitung durch die verantwortliche Stelle bis zur Auskunftserteilung, ist sicherlich reizvoll. Die datenschutzrechtlichen Vorgaben stellen an solche Konzepte hohe Anforderungen, beispielweise in Zusammenhang mit der Authentisierung des Anfragenden und Verifizierung der Zustelladresse. Die derzeit geringe Verbreitung des nPA und kostenintensive Entwicklungsarbeit dürften solche Lösungen derzeit unattraktiv wirken lassen. Der Medienbruch innerhalb einer nicht volldigitalisierten Abwicklung der Auskunft bietet jedoch auch Vorteile. Durch geeignete Maßnahmen können die ökonomischen Nachteile zudem drastisch minimiert werden. Zudem ist es wenig substanziell, Konzepten, die den Datenaustausch mittels Postversand organisiert haben, per se einen zeitlichen Nachteil zu unterstellen. Einem globalen Wirtschaftssystem dürfte zugetraut werden, gut funktionierende Logistikketten etabliert zu haben.[39]

Ein Medienbruch besteht, wenn Auskunftsersuchen über das Portal erzeugt, ausgedruckt, mit einer Unterschrift versehen und per Post zu der verantwortlichen Stelle gesendet werden. Diese wird es intern bearbeiten, ggf. digitalisieren, um es in den Systemen der Organisation zu verarbeiten, und die Auskunft ebenfalls per Post an den Verbraucher senden. Der Medienbruch in Form des Postversands bietet den Vorteil, dass die verantwortliche Stelle ein Auskunftsersuchen mit einer Unterschrift erhält, auch wenn diesbezüglich keine gesetzliche Formvorgabe besteht (vgl. 2.3.1). Beide Beteiligte dürfen bei dem Versand von personenbezogenen Daten auf den Schutz durch das Briefgeheimnis vertrauen.[40] Zusätzlich dürften die anfallenden Portokosten Auskunftsersuchen weitestgehend auf die Fälle beschränken, in denen ein tatsächliches Interesse an einer Auskunft besteht. Die Beantwortung des Auskunftsersuchens durch das Unternehmen per Post bietet im Gegensatz zur elektronischen Übermittlung den Vorteil, dass keine technischen Maßnahmen zur sicheren Übertragung implementiert werden müssen. Die Entwicklung und der Einsatz neuer elektronischer Übermittlungskonzepte, die das bestehende Schutzniveau übertreffen, sind zwar wünschenswert. Die unverschlüsselte E-Mail-Kommunikation wird dieser Anforderung aber nicht gerecht.

In den Auskunftsprozess können jedoch Maßnahmen integriert werden, die die ökonomischen Nachteile des Medienbruchs abschwächen. Auskunftsersuchen, die von Betroffenen in einem Auskunftsportal erstellt werden, sollten klar strukturiert sein, damit die verantwortliche Stelle sie für die interne Bearbeitung problemlos mittels Texterkennung digital erfassen kann und nicht manuell erfassen muss. Weitere Maßnahmen zur Unterstützung bei der Digitalisierung sind denkbar. Es können etwa leicht auslesbare Codes bei der Erstellung in das Auskunftsersuchen integriert wer-

[39] Die Brieflaufzeiten der Deutschen Post AG werden innerhalb Deutschlands mit einem Tag angegeben. Nach Angaben der Deutsch Post AG trifft diese Aussage für 95 % der Sendungen zu. http://www.deutschepost.de/dpag?tab=1&skin=hi&check=yes&lang=de_DE&xmlFile=link1022896_1022864 (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

[40] Siehe § 202 StGB.

den. Dies kann beispielsweise ein QR-Code[41] sein, der Adress-, Identifikationsdaten und Angaben über die Art des Ersuchens enthält.[42]

5.5 Zentrale Datenverarbeitung im Portal

Für Nutzerinnen und Nutzer eines Auskunftsportals können persönlichkeitsrechtliche Risiken durch die zentrale Stellung eines solchen Dienstleisters bestehen. Auch wenn ein zentrales Angebot durch die Bündelung der Informationen über das Auskunftsrecht und die konkreten Möglichkeiten, das Recht bei den verantwortlichen Stellen geltend zu machen, praktisch für Betroffene ist, birgt jede zentrale Position in einer organisatorischen oder technischen Architektur das Risiko einer Verkettung aller dort anfallenden Daten. Bei einem Auskunftsportal betrifft dies nicht nur die durch den Internet-Zugriff technisch bedingt anfallenden Daten sowie Informationen über die Nutzung des Portals; der Dienstleister kann bei dem Versand von Auskunftsersuchen auch Kenntnis von Inhalten und Adressaten der Auskunftsbegehren erhalten. Dies lässt Rückschlüsse auf spezifische Interessen und mutmaßliche Kontakte der Betroffenen zu. Die Informationen können sich zu Persönlichkeitsprofilen verdichten, das immer detaillierter wird, wenn erneut Auskunftsbegehren verschickt werden. Durch die Vergleichbarkeit des Auskunftsverhaltens verschiedener Nutzerinnen und Nutzer können sich die persönlichkeitsrechtlichen Risiken erhöhen. Diese Risiken lassen sich eindämmen, indem Strukturen genutzt werden, in denen der Dienstleister nur als „Bote" agiert, ohne von den Inhalten und Adressaten der Auskunftsersuchen Kenntnis zu erhalten (vgl. 6.2.2.1).

Äußerst weitreichende Kenntnisse erhielte ein Dienstleister, der zusätzlich mit dem Empfang der Auskunft beauftragt würde (vgl. 6.2.2.2). Es ist fraglich, welchen Mehrwert dies für den Betroffenen bieten soll. Jedenfalls ist die Erhebung und Speicherung der Auskunft bei einem Dienstleister nicht erforderlich. Eine Überprüfung der gespeicherten Daten auf Richtigkeit kann nur der Betroffene selbst vornehmen. Seriöse Dienstleister werden daher eine eigene Möglichkeit der Kenntnisnahme ausschließen.

5.6 Auskunftsportal als unternehmensspezifische Lösung

Ein Auskunftsportal ist auch als spezifische Lösung zur Kanalisierung der Auskunftsersuchen und evtl. verwandter Anfragen an eine bestimmte Organisation wie etwa ein Unternehmen denkbar. Es wäre somit ein Auskunftsportal für ein spezifisches Unternehmen. Betroffene, die ein Auskunftsersuchen stellen oder allgemeine Informationen über die Datenverarbeitung in diesem Unternehmen erhalten möchten, können sich an das Auskunftsportal dieses Unternehmens wenden. Dabei wird das Auskunftsportal unter der Leitung und Kontrolle der verantwortlichen Stelle betrieben. Betroffene wenden sich für ein Auskunftsersuchen so „direkt" an die verantwortliche Stelle. In diesem Fall ist kein Dritter in den Auskunftsprozess eingeschaltet. Die Problematik einer zentralen Datenhaltung in einem allgemeinen Auskunftsportal ist in diesem Fall nicht relevant (vgl. 5.5).

---

41 Kurzform von Quick Response Code.

42 Bei der Nutzung von Codes sollte Betroffenen erklärt werden, welche Daten sich in dem Code verbergen. Eine solche Transparenzmaßnahme fördert die Akzeptanz solcher Verfahren.

Ein solches spezifisches Auskunftsportal bietet einer verantwortlichen Stelle die Möglichkeit, in besonderer Weise Engagement in Datenschutzfragen zu zeigen, über die eigene Datenverarbeitung umfassend zu informieren und Anfragen Betroffener dadurch zuvorzukommen. Auch in dieser Ausprägung eines Auskunftsportals können die wesentlichen Vorteile genutzt werden. Die Identifikationsdaten, die für die Beantwortung des Auskunftsersuchens erforderlich sind, können strukturiert erhoben und einfacher in die unternehmensinternen Prozesse eingesteuert werden. Das spezifische Auskunftsportal bildet somit wieder den Beginn der Prozesskette „Auskunftsersuchen".

6 Anforderungen an ein Auskunftsportal

Ein Online-Auskunftsportal bietet seine Dienste im Internet an. Internetdienste haben vor allem die Vorgaben der bereichsspezifischen Vorschriften des TMG und des TKG zu beachten sowie ergänzend die des BDSG. So finden gem. § 1 Abs. 3 BDSG die Vorgaben des BDSG Anwendung, wenn bestimmte Fragen des Datenumgangs nicht in den bereichsspezifischen Vorschriften speziell geregelt werden. Je nach Ausgestaltung der angebotenen Dienste ist zu prüfen, welche Normen in welchem Umfang zur Anwendung kommen.

Telemediendienste sind gem. § 1 Abs. 1 Nr. 1 TMG elektronische Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste, telekommunikationsgestützte Dienste oder Rundfunk sind. Darunter fallen insbesondere Internetseiten und andere Internetangebote, auch wenn sie beispielsweise Meinungsforen umfassen.[43] Ein Online-Auskunftsportal stellt daher einen Telemediendienst dar. Der Betreiber eines Auskunftsportals ist Diensteanbieter i. S. d. § 2 S. 1 Nr. 1 TMG. Es ist eine natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält. Es finden die Vorschriften des TMG Anwendung. Insbesondere sind die Datenschutzbestimmungen des vierten Abschnitts des TMG zu beachten. Das TMG findet gem. §§ 14, 15 TMG ausschließlich für Bestands- und Nutzungsdaten Anwendung. Für Inhaltsdaten, d. h. inhaltliche Angaben zur Ausgestaltung der Telemedien, die nicht für die Bereitstellung von Telemedien erforderlich sind, sieht das TMG keine bereichsspezifische Regelung vor. Auf Inhaltsdaten findet daher bei Vorliegen der weiteren Voraussetzungen das BDSG Anwendung.

Telekommunikationsdienste sind gem. § 3 Nr. 24 TKG Dienste, die in der Regel gegen Entgelt erbracht werden sowie ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen und umfassen auch Übertragungsdienste in Rundfunknetzen. Telekommunikation stellt gem. § 3 Nr. 22 TKG die technischen Vorgänge des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen dar. Dies betrifft jede moderne Form der Kommunikation.[44] Unter Telekommunikationsdienste fallen Nachrichtendienste wie Telefonie, Mobilfunk und E-Mail, aber auch die Bereitstellung der Nutzung des Internets. Besonders geschützt durch das Fernmeldegeheimnis sind nach § 88 TKG sowohl der Inhalt als auch die näheren Umstände der Kommunikation. Bietet ein Auskunftsportal Telekommunikationsdienste wie E-Mail an, hat es die Vorgaben des TKG zu beachten. Teil 7 des Gesetzes enthält spezielle datenschutzrechtliche Vorgaben.

[43] Moos in Taeger / Gabel, Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 1. Auflage, 2010, TMG Einführung, Rn. 5.

[44] Munz in Taeger / Gabel, Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 1. Auflage, 2010, TKG Einführung, Rn. 7.

6.1 Allgemeine Anforderungen an ein Auskunftsportal

6.1.1 Transparenz

Ein Online-Auskunftsportal verfolgt das Ziel, Verbraucherinnen und Verbraucher bei der Wahrnehmung ihrer Datenschutzrechte zu unterstützen. Es ist davon auszugehen, dass die relevante Zielgruppe erhöhte Aufmerksamkeit auf die Einhaltung der Datenschutzvorschriften richtet. Erfahrungsgemäß wird besonders die Einhaltung von Transparenzvorgaben (vgl. 2.1.9) beobachtet. Eine Überprüfung der Einhaltung dieser Vorgaben ist verhältnismäßig einfach möglich. Zuspruch wird ein Online-Auskunftsportal daher nur erlangen können, wenn es Nutzerinnen und Nutzer in vorbildlicher Weise über die Verwendung personenbezogener Daten informiert. Die Vorbildlichkeit kann beispielsweise in einer besonderen Verständlichkeit und Übersichtlichkeit der Transparenzangebote bestehen. Eine besondere Attraktivität kann ein Angebot erlangen, wenn zu Gunsten der Verbraucherfreundlichkeit über die gesetzlichen Mindestvorgaben hinausgegangen wird.

Zu jedem Verfahren der automatisierten Verarbeitung personenbezogener Daten ist ein Verfahrensverzeichnis zu erstellen (vgl. 6.2.3.2). Um eine effektive Kontrolle nicht zuletzt für die verantwortliche Stelle selbst aber beispielsweise auch für die Datenschutzaufsichtsbehörde zu ermöglichen, sollten über die Vorgaben des § 4e BDSG hinausgehende, wesentliche Informationen aufgenommen werden. Dazu gehören unter anderem die konkreten Datenempfänger sowie die Rechtsgrundlagen der jeweiligen Datenverwendung.

Verantwortliche Stellen haben Betroffene bei der Erhebung personenbezogener Daten nach § 4 Abs. 3 BDSG über die Identität der verantwortlichen Stelle, die Zweckbestimmung der Datenverwendung und die Kategorien von Empfängern zu unterrichten, sofern diese nicht bereits auf andere Weise Kenntnis erlangt haben. Besondere Unterrichtungspflichten bestehen nach § 13 Abs. 1 TMG. Danach ist zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung der Daten in Staaten außerhalb des Anwendungsbereichs der EG-Datenschutzrichtlinie in allgemein verständlicher Form zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. Außerdem ist zu Beginn eines automatisierten Verfahrens, das eine spätere Identifizierung ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, zu unterrichten. Der Inhalt der Unterrichtung muss jederzeit abrufbar sein.

Bietet der Betreiber des Auskunftsportals Telekommunikationsdienste wie E-Mail-Dienste an, etwa um Auskunftsersuchen an Unternehmen zu übermitteln, sind die Teilnehmer gem. § 93 TKG bei Vertragsabschluss über Art, Umfang, Ort und Zweck der Erhebung und Verwendung personenbezogener Daten so zu unterrichten, dass sie in allgemein verständlicher Form Kenntnis von den grundlegenden Verarbeitungstatbeständen der Daten erhalten. Dabei sind sie auch auf die zulässigen Wahl- und Gestaltungsmöglichkeiten hinzuweisen. Die Informationen über die Erhebung und Verwendung personenbezogener Daten müssen allgemein zugänglich sein. Zudem müssen die Teilnehmer über Fälle, in denen ein besonderes Risiko der Verletzung der Netzsicherheit besteht, informiert werden.

Werden Einwilligungen eingeholt, müssen Betroffene gem. § 4a Abs. 1 S. 2 BDSG auf den Zweck der Datenverwendung und gegebenenfalls auf die Folgen einer Verweigerung der Einwilligung hingewiesen werden. Der Betreiber eines Online-Auskunftsportals kann als Diensteanbieter gem. § 13 Abs. 2 TMG Einwilligungen elektronisch einholen, wenn sichergestellt ist, dass Nutzerinnen und Nutzer die Einwilligungen bewusst und eindeutig erteilen, die Einwilligungserklärungen protokolliert werden, jederzeit abrufbar sind und mit Wirkung für die Zukunft widerrufen werden können. Der Betreiber hat die Nutzerinnen und Nutzer gem. § 13 Abs. 3 TMG vor der Erklärung der Einwilligung auf das Widerrufsrecht hinzuweisen. Dieser Hinweis muss jederzeit abrufbar sein.

6.1.2 Benutzungsfreundlichkeit

Ziel eines Auskunftsportals ist es, eine möglichst große Zielgruppe anzusprechen und diese effektiv bei der Wahrnehmung der datenschutzrechtlichen Auskunftsrechte zu unterstützen. Dieses Ziel kann nur erreicht werden, wenn das Portal möglichst selbsterklärend gestaltet ist. Es sollte durch eine zielgruppenorientierte Ansprache zur Benutzung einladen. Zur Vereinfachung und zur Benutzerfreundlichkeit können die Reduzierung von Text und/oder die Illustration anhand von Symbolen und Graphiken beitragen. (Datenschutz-)Rechtliche Sachverhalte sollten zunächst vereinfacht und verständlich, allerdings mit einer konkreteren Vertiefungsmöglichkeit dargestellt werden. Auf der Vertiefungsebene sollten ggf. die gesetzlichen Regelungen und Hintergründe dargestellt werden. Außerdem können an dieser Stelle Links zu weiteren vertiefenden Inhalten angeboten werden.

Auf Benutzungsfreundlichkeit ist in besonderer Form zu achten, wenn Nutzerinnen und Nutzern Wahlmöglichkeiten bei der Benutzung des Dienstes geboten werden. Stehen etwa zwei Nutzungsalternativen zur Erreichung eines Zwecks zur Verfügung, müssen für beide im Rahmen des Stands der Technik möglichst unkomplizierte Zugangsmöglichkeiten angeboten und erläutert werden. Die Erläuterung sollte wertneutral und verständlich erfolgen. Außerdem sollten die Alternativen gleichwertig, d. h. auch optisch äquivalent, dargestellt werden. So sollte etwa in der Benutzerführung der grundlegende Hinweis auf die Alternativen generell auf einer Bildschirmseite und innerhalb derer ausgeglichen prominent erfolgen. Es sollte vermieden werden, etwa eine Alternative als nachrangig darzustellen, indem sie etwa im unteren Bildschirmbereich oder sogar erst durch Scrollen wahrnehmbar ist. Relevanz erhält die äquivalente Darstellung von Wahlmöglichkeiten insbesondere im Bereich der einwilligungsbasierten Datenverwendung, da diese eine freiwillige Entscheidung des Betroffenen erfordert (vgl. 6.2.1.2).

6.1.3 Informationsangebot eines Auskunftsportals

Die Unterstützung bei der Wahrnehmung datenschutzrechtlicher Auskunftsrechte sollte effektiv und im Sinne einer möglichst generellen Wirkung auch als „Hilfe zur Selbsthilfe“ erfolgen. Dieser Ansatz kann verwirklicht werden, indem das Auskunftsportal als „zentraler Anlaufpunkt“ zu Fragen der Auskunftsrechte und ggf. weiterer Datenschutzaspekte ein umfassendes und aussagekräftiges Informationsangebot zur Verfügung stellt.

Ein wichtiger Teil dieses Angebots sind Informationen über Unternehmen, die personenbezogene Daten verarbeiten. Dieses Angebot kann sowohl Informationen umfassen, die von Unternehmen zu ihren konkreten Datenverarbeitungsvorgängen bereit gestellt werden (vgl. 6.1.3.1), als auch eine Übersicht zu datenverarbeitenden Unternehmen beispielsweise sortiert nach Branchen. Die zuletzt genannte Übersicht erscheint für die Attraktivität und Effektivität eines Portals von essentieller Bedeutung, da bei Verbraucherinnen und Verbrauchern erfahrungsgemäß kein Überblick über die Vielfalt der datenverarbeitenden Unternehmen, die Einordnung in Branchen und mögliche Zusammenhänge zwischen bestimmten Unternehmen bzw. Branchen besteht. Gleichwohl besteht ein Bedürfnis bei Verbraucherinnen und Verbrauchern, einen Überblick über Datenflüsse zu erlangen. Ein berechtigtes Interesse von Unternehmen, in diesem Kontext nicht genannt zu werden, um nicht Adressat vermehrter Auskunftsersuchen zu werden, ist nicht ersichtlich. Denn für Unternehmen bestehen beispielsweise Publizitätspflichten etwa nach dem Handelsgesetzbuch (HGB), was ihr besonderes Verhältnis zu Öffentlichkeit, insbesondere im Interesse der Funktionsfähigkeit des Rechtsverkehrs, unterstreicht. Der Schutz von Betriebs- und Geschäftsgeheimnissen[45] bleibt von den Publizitätspflichten unberührt. Im Übrigen werden Unternehmen nicht durch ein mit dem Recht auf informationelle Selbstbestimmung vergleichbaren Recht geschützt. Jedenfalls sind die Interessen der Bürgerinnen und Bürger, sich Informationen zur Wahrnehmung ihrer Datenschutz- und somit ihrer Grundrechte zu verschaffen, als sehr hochwertig einzuschätzen.

Daneben kann ein Auskunftsportal Informationen über rechtliche Aspekte der Auskunftsersuchen zur Verfügung stellen (vgl. 6.1.3.2). Hierzu bestehen bei Verbraucherinnen und Verbrauchern erfahrungsgemäß zahlreiche Fragen. Denn die Wahrnehmung von Datenschutzrechten gehört nicht zu den alltäglichen Vorgängen und die rechtliche Lage stellt sich nicht übersichtlich dar. Es hat sich praktisch bewährt, häufig auftretende Problemstellungen in der Form von „Frequently Asked Questions“ (FAQ) zu behandeln und die Antworten auf diesem Weg für eine breite Öffentlichkeit auffindbar zu machen. Ergänzt werden könnte dies durch ein Glossar, das zentrale Begrifflichkeiten verständlich erläutert.

Ein solches umfassendes Informationsangebot könnte zudem die Attraktivität und Bekanntheit des Auskunftsportals erhöhen. Voraussetzung hierfür ist allerdings, dass Aktualität und Zuverlässigkeit der Informationen sichergestellt sind. Hierfür müssen organisatorische Strukturen verbindlich festgelegt und eingerichtet werden, wie insbesondere ein konkreter Prüfturnus und entsprechende Zuständigkeiten. Sollten veraltete oder falsche Informationen angeboten werden, könnte dies einen erheblichen Imageschaden für ein Auskunftsportal in Form eines Vertrauensverlustes zur Folge haben. Verbraucherinnen und Verbraucher müssen dem Portal allerdings vertrauen können, um es bei der Wahrnehmung ihrer Auskunftsrechte zu nutzen.

Ein in der dargestellten Form abgesichertes Informationsangebot könnte sowohl für die Verbraucherinnen und Verbraucher als auch für Unternehmen den Vorteil bieten, dass Fragen im Vorfeld geklärt und Anfragen obsolet werden. Für den Fall, dass eine Anfrage gestellt wird, könnten bei-

[45] Der Schutz von Betriebs- und Geschäftsgeheimnissen knüpft an Art. 12 und Art. 14 GG an, BVerfG-Urteil vom 24.11.2010, Az. 1 BvF 2/05, Rz. 204, 208.

spielsweise Missverständnisse oder andere Verzögerungsgründe ausgeschlossen werden, indem neutral über Begrifflichkeiten, Formerfordernisse und Abläufe unterrichtet wird.

Bewertungen und Statistiken sind erfahrungsgemäß für die Öffentlichkeit ebenfalls von einem gewissen Interesse. Bewertungen stellen in der Regel Meinungsäußerungen dar. Sie können etwa in Form standardisierter Fragen mit einer vordefinierten Antwortskala, aber auch als Freitext erfolgen, und beispielsweise die Verständlichkeit von Auskünften betreffen. Statistiken werden (in diesem Kontext unabhängig von der wissenschaftlichen Bedeutung des Begriffs) Aussagen unabhängig von dem einzelnen Auskunftsersuchen zusammenfassen. Sie können etwa die Anzahl von Auskunftsersuchen an ein bestimmtes Unternehmen insgesamt, die Anzahl unvollständiger Auskünfte innerhalb einer Branche oder die durchschnittliche Beantwortungsdauer darstellen. Es stellt sich jedoch die Frage, wie valide Informationen erhoben werden können. Um beispielsweise eine Aussage über die Anzahl von Anfragen an ein Unternehmen treffen zu können, müsste ein Auskunftsportal diesbezüglich Informationen erheben bzw. informiert werden. Die Information könnte es etwa erlangen, wenn es in die Versendung des Auskunftsersuchens eingebunden ist (was datenschutzrechtlich nicht unbedenklich ist, vgl. 5.5). Es muss sichergestellt sein, dass bei dem Einsatz von Statistik- und Bewertungsfunktionen der Datensparsamkeitsgrundsatz (vgl. 2.1.4) beachtet wird, also möglichst anonymisierte Daten verwendet werden (vgl. 6.2.1.5).

6.1.3.1 Unternehmen

Für Unternehmen könnte ein Auskunftsportal die Möglichkeit bieten, zentral und prominent Informationen für Verbraucherinnen und Verbraucher zur Verfügung zu stellen. Je detaillierter, relevanter und verständlicher die Informationen aufbereitet sind, desto höher ist die Wahrscheinlichkeit, dass Verbraucherinnen und Verbraucher ihre Fragen beantwortet sehen und sich ein Auskunftsersuchen für sie erledigt. So könnten beispielsweise Informationen über die in dem Unternehmen etablierten Datenverarbeitungsverfahren verbraucherfreundlich aufbereitet und dargestellt werden, um einen detaillierten Überblick über die regelmäßig stattfindenden Datenflüsse zu gewähren. Da sich erfahrungsgemäß viele Fragen auf die Rechtsgrundlage der Verwendung, die Herkunft und die Speicherdauer von Daten richten, dürfte sich eine genaue Information hierzu als effektiv erweisen. Unternehmensindividuell könnten zudem häufig gestellte Fragen vorweggenommen werden.

Dieser Effekt hängt maßgeblich davon ab, dass die Informationen von Verbraucherinnen und Verbrauchern als seriös und zuverlässig wahrgenommen werden. Hierzu kann die Einbindung in den Rahmen eines neutralen Portals beitragen. Die Richtigkeit und Aktualität der Unternehmensinformationen kann allerdings nur das Unternehmen selbst sicherstellen. Insofern sind die Verantwortlichkeiten klar dem Unternehmen zuzuweisen beispielsweise in den Allgemeinen Geschäftsbedingungen, die für die Vertragsverhältnisse zwischen dem Portal und den teilnehmenden Unternehmen gelten. Diese Verantwortlichkeiten sind auch bei der Gestaltung des Portals abzubilden. Dies kann z. B. durch eine farbige Hinterlegung der Unternehmensinformationen in Verbindung mit einem Hinweis auf die Verantwortlichkeit des Unternehmens für die Inhalte erfolgen. Empfehlenswert ist es, an dieser Stelle einen Kontaktweg zur Meldung von Fehlern wie veralteten Inhalten

anzubieten. Fehler der Unternehmensinhalte würden von Nutzerinnen und Nutzern dem Portal zugerechnet werden. Dies kann auch dann nicht sicher ausgeschlossen werden, wenn ein Hinweis auf die Verantwortlichkeit des Unternehmens erfolgt. Daher sollten die Meldungen neben dem Unternehmen auch dem Portal zugehen. Denn die Glaubwürdigkeit und der Erfolg des Portals insgesamt hängen davon ab, dass nur richtige und aktuelle Informationen angeboten werden. Das Verfahren zur Bearbeitung von Fehlermeldungen muss daher – wie im Fall des anlasslosen Prüfturnuses (vgl. 6.1.3) – verbindlich festgelegt sein. Insbesondere muss die Pflicht für das Unternehmen statuiert sein, Meldungen unverzüglich zu bearbeiten und Fehler zu beheben. Auch hierfür bieten sich die vertraglichen Vereinbarungen zwischen Portal und teilnehmenden Unternehmen an.

Im Interesse des Renommees des Portals sollten in den vertraglichen Vereinbarungen mit den Unternehmen Mindestanforderungen an die zur Verfügung gestellten Informationen festgelegt werden. So sollte etwa grundsätzlich die Verpflichtung bestehen, die Informationen zu den Datenverarbeitungsvorgängen in einem Unternehmen vollständig und nach bestimmten feststehenden Kategorien bzw. Kriterien darzustellen. Wenn ausnahmsweise keine vollständigen Informationen zur Verfügung gestellt werden, sollte die Verpflichtung bestehen, auf die Unvollständigkeit und darauf, welche konkreten Punkte dies betrifft, hinzuweisen.

6.1.3.2 Rechtliche Aspekte

Für Verbraucherinnen und Verbraucher gehört die Geltendmachung datenschutzrechtlicher Auskunftsansprüche nicht zu den alltäglichen Vorgängen. Hinzu kommt, dass gesetzliche Hintergründe nicht im Detail bekannt sind und die befürchteten Formalismen eine „abschreckende Wirkung“ haben (zu Informationsdefiziten und Ausführungshindernissen vgl. 3.2). Dementsprechend benötigen Verbraucherinnen und Verbraucher verständliche Informationen, die sie bei der Geltendmachung ihrer Auskunftsrechte unterstützen. Dies umfasst insbesondere eine Erklärung dessen, welche Angaben der Auskunftsanspruch umfasst, aus welcher Rechtsvorschrift er sich ergibt, gegen wen er geltend gemacht werden kann und ob Formvorgaben bestehen. Außerdem können grundlegende Informationen zu datenschutzrechtlichen Fragestellungen, Gesetzen und Begrifflichkeiten angeboten werden. Hilfreich erscheint es auch, Informationen zu einem effektiven und zielorientierten Vorgehen, etwa zur Adressierung an den betrieblichen Datenschutzbeauftragten, zur Fristsetzung und zur Hinterlegung einer Kopie des Auskunftsersuchens bei den eigenen Unterlagen, bereitzustellen. Sollte ein Musteranschreiben (vgl. 6.1.3.3) angeboten werden, sollte diesem ebenfalls eine Information zum vorgesehenen Verfahrensablauf, also etwa die Fertigung einer Kopie für die eigenen Unterlagen, das Notieren der Frist sowie der eigenverantwortliche Versand, zur Klarstellung angehängt werden. In einem allgemeinen Informationsbereich können zudem Informationen über Eskalationsmöglichkeiten bei Ausbleiben von Auskünften dargestellt werden (vgl. 3.4). Außerdem könnten Inhalte zu verwandten Themen wie die Wahrnehmung von Berichtigungs- und Löschansprüchen und von weiteren Betroffenenrechten aufgenommen werden.

6.1.3.3 Musteranschreiben

Eine erfahrungsgemäß willkommene Erleichterung besteht in dem Bereitstellen eines Musteranschreibens zur Wahrnehmung des Auskunftsanspruchs. Hierdurch kann der Befürchtung, Formvorgaben nicht einzuhalten, begegnet werden. Generell kann mit diesem Hilfsmittel das Hemmnis, ein Schreiben zu formulieren, abgebaut werden.

Der systematisch grundlegende und grundsätzlich umfassende Auskunftsanspruch nach § 34 Abs. 1 BDSG sollte Gegenstand eines grundlegenden Musteranschreibens sein (vgl. 4.1.1). Schränkt der Anfragende sein Auskunftsersuchen nicht ein, ist Auskunft über alle zu seiner Person gespeicherten Daten zu erteilen (vgl. 2.3.1). Den Nutzerinnen und Nutzern des Auskunftsportals sollte die Möglichkeit geboten werden, die Anschreiben zu konkretisieren. In diesem Zusammenhang könnte es einen besonderen Service darstellen, Konkretisierungsvorschläge – auch zur Illustration der möglichen Datenverarbeitungsverfahren – anzubieten. So könnten etwa Textbausteine zur Verfügung gestellt werden, wonach der Anfragende als Bewerber, Mitarbeiter, Lieferant, Kunde, Interessent und/oder Webseitenbesucher mit der verantwortlichen Stelle in Kontakt gestanden hat und um Auskunft zu in diesem Kontext verwendeten Daten bittet. Eine Konkretisierung der Anfrage könnte auch anhand bestimmter Datenkategorien wie Kundendaten, Bonitätsdaten, besondere Arten personenbezogener Daten (vgl. 2.2), Werbedaten oder Nutzungsprofildaten erfolgen. Neben dieser Einschränkung des Auskunftsersuchens, könnte es zudem einen Mehrwert für Anfragende und angefragte Stelle darstellen, eine Möglichkeit zur Konkretisierung des Sachverhalts zu schaffen. Dabei könnte der Umstand berücksichtigt werden, dass verantwortliche Stellen zum Teil keinen Überblick über alle Datenverarbeitungsverfahren haben, in denen Daten des Anfragenden verwendet worden sein können. Anfragenden könnte etwa die Möglichkeit geboten werden, Bestellverfahren o. Ä. detailliert zu schildern oder beispielhaft auf ihnen bereits bekannte Datenempfänger wie Reichweitenanalysedienste oder Kooperationspartner hinzuweisen. Es ist empfehlenswert diesbezüglich einen Textbaustein zur Verfügung zu stellen, wonach es sich nur um beispielhafte Aufzählungen handelt und keine auf diese Schilderung beschränkte, sondern eine umfassende Auskunft verlangt wird. Da nicht alle Konstellationen vorweggenommen werden können, wird daneben ein Freitextfeld angeboten werden müssen.

Da unterschiedliche Auskunftsansprüche bestehen (vgl. 2.3.1), sollten Bausteine für das Musteranschreiben bereit gestellt werden. Über das Portal müssen die Nutzerinnen und Nutzer verständlich zu der Auswahl der für ihr Anliegen vorgesehenen Bausteine geführt werden (vgl. 6.1.2). Eine effektive Benutzerführung könnte über eine Liste von Anlässen (vgl. 3.1) oder Adressaten leiten. Je nach Branche bzw. Datenverarbeitungskategorie der Vorauswahl könnten die entsprechenden Bausteine vorgeschlagen werden. Würde beispielsweise als Adressat eines Auskunftsersuchens eine Auskunftei gem. § 29 BDSG ausgewählt, so müsste jedenfalls ein Baustein für ein Auskunftsersuchen gem. § 34 Abs. 4 BDSG zu den zum Anfragenden berechneten Wahrscheinlichkeitswerten angeboten werden. Sollte eine solche Auswahlfunktion und Benutzerführung nicht vorgesehen werden, ist jedenfalls informativ darauf hinzuweisen, falls die Auskunftsvorschrift einen spezifischen Antrag des Betroffenen verlangt (durch den Gesetzeswortlaut „auf Verlangen“). Nutzerinnen und Nutzer sollten die Möglichkeit haben, die Bausteine nach ihren Bedürfnissen auszuwählen und zusammenzustellen.

6.1.3.4 Vergabe eines Gütesiegels durch ein Auskunftsportal

Eine besondere Form der Information durch das Auskunftsportal könnte die Vergabe eines Gütesiegels für die Auskunftsprozesse von Unternehmen sein. An Gütesiegel, die auch andere Bezeichnungen tragen können, aber jedenfalls als Qualitätszertifikat in Erscheinung treten, werden entsprechend ihrer zunehmenden Bedeutung und insbesondere ihrer Werbewirksamkeit allerdings hohe Anforderungen gestellt. Sie werden vom Rechtsverkehr nur bei einer sachgerechten Prüfung durch eine neutrale Instanz anerkannt.[46]

Neutralität ist nicht mit wirtschaftlichen Abhängigkeiten vereinbar. An einer unabhängigen Begutachtung fehlt es, wenn für das Führen der in dem Siegel liegenden Empfehlung Lizenzgebühren zu entrichten sind. Das Wesen einer Lizenzgebühr besteht darin, dass der Lizenznehmer (nur) für die Berechtigung zur Nutzung eines gewerblichen Rechts ein Entgelt zahlt. Die Kosten für tatsächliche Prüfungen, Testkäufe o. Ä. können dagegen in einem Zertifizierungsverfahren durch die Erhebung von entsprechenden Gebühren gedeckt werden.[47] Hat eine Zahlung innerhalb eines Zertifizierungsverfahrens den Charakter einer Gebühr nach sachlicher Prüfung der Voraussetzungen wie beispielsweise durch eine unabhängige Jury, wird dies als zulässig angesehen.[48] Neben der wirtschaftlichen Unabhängigkeit dürfen auch keine sonstigen Anhaltspunkte für einen Mangel an Neutralität bestehen.

Eine sachgerechte Prüfung kann nur durch fachkundige Experten sichergestellt sein. Im datenschutzrechtlichen Kontext müssen diese sowohl die entsprechende rechtliche als auch die technische Fachkunde aufweisen. Zudem dürfen keine Zweifel hinsichtlich der Zuverlässigkeit und Unabhängigkeit bestehen. Eine sachgerechte Prüfung erfordert zudem, dass eine qualifizierte Beurteilung von Tatsachen nach einheitlichen Kriterien vorgenommen wird.[49] Zur Qualitätssicherung und insbesondere zur Sicherstellung der Einheitlichkeit der Prüfpraxis hat es sich bewährt, das Prüfergebnis durch eine unabhängige Zertifizierungsstelle bestätigen zu lassen.

Der Zertifizierungsumfang muss klar bestimmt sein und die wesentlichen Erwartungen an die Qualitätsaussage der Zertifizierung erfassen. Nur wenn der Zertifizierungsumfang hinreichend klar bestimmt ist, können entsprechende Prüfkriterien festgelegt werden. Die Prüfkriterien müssen im Hinblick auf den Zertifizierungsumfang relevant sein. Von besonderer Bedeutung ist, dass die Einhaltung der Kriterien die Einhaltung der zu beachtenden Vorschriften erleichtern muss. Werden Anforderungen über die gesetzlichen Anforderungen hinaus gestellt, sind – nicht zuletzt zur Gewährleistung einer einheitlichen Prüfpraxis – diese Anforderungen detailliert und in einer prüffähigen Form zu bestimmen. Das heißt, es darf kein erheblicher Ermessensspielraum bei der Auslegung der Anforderungen bestehen.

---

[46] OLG Frankfurt, Beschluss vom 08.03.1994, Az. 6 W 16/94; OLG Dresden, Urteil vom 03.07.2012, Az. 14 U 167/12.

[47] LG Darmstadt, Urteil vom 24.11.2008, Az. 22 O 100/08.

[48] BGH, Urteil vom 04.10.1990, Az. I ZR 39/89.

[49] LG Köln, Urteil vom 05.01.2012, Az. 31 O 491/11.

Der Rechtsverkehr muss in ausreichendem Maße über das Zustandekommen eines Gütesiegels aufgeklärt werden.[50] Neben Informationen zum Zertifizierungsprozess und den allgemeinen Prüfkriterien müssen auch die wesentlichen Ergebnisse eines konkreten Zertifizierungsverfahrens, beispielsweise in Form eines Kurzgutachtens, veröffentlicht werden.

6.2 Auskunftsportal als datenverarbeitende Stelle

6.2.1 Datenerhebung und -verarbeitung durch das Auskunftsportal

Werden über ein Online-Auskunftsportal Formulare zum Erstellen von Auskunftsersuchen angeboten und die anzugebenden Daten durch den Betreiber gespeichert und werden Zusatzdienste wie E-Mail-Erinnerungen angeboten, werden personenbezogene Daten verwendet. Zudem sind Nutzerinnen und Nutzer über IP-Adressen bestimmbar, weshalb sie nach herrschender Auffassung personenbeziehbare Daten[51] darstellen.

6.2.1.1 Voraussetzungen

Als grundlegende datenschutzrechtliche Maßgabe ist zu beachten, dass für die automatisierte Datenverwendung ein generelles Verbot mit Erlaubnisvorbehalt gilt (vgl. 2.1.3). Die Verwendung personenbezogener Daten sowie die Auswahl und Gestaltung von Datenverarbeitungssystemen sind gem. § 3a BDSG außerdem an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen (vgl. 2.1.4). Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert. Bei der Planung und Konzeption von Verfahren sollte generell geprüft werden, ob Privacy-Enhancing Technologies (PET) eingesetzt werden können. Grundsätzlich dürfen nur die Daten verwendet werden, die zur Bereitstellung des Dienstes und ggf. zu Abrechnungszwecken erforderlich sind.

Ein Auskunftsportal sollte in jeder Hinsicht vorbildlich die informationelle Selbstbestimmung der Nutzerinnen und Nutzer nicht nur respektieren, sondern auch aktiv unterstützen. Generell anzustreben sind daher Verfahren bzw. Prozesse, die auf die Verwendung personenbezogener Daten durch das Portal selbst bzw. den Betreiber verzichten. Denkbar sind hier etwa Lösungen, die es Betroffenen ermöglichen, Auskunftsersuchen auf ihrem eigenen Client zu verwalten, und im Rahmen derer beispielsweise nur die Musteranschreiben zum Herunterladen bereitgestellt werden. Wenn doch Verfahren bzw. Prozesse aufgesetzt werden, die eine Verwendung personenbezogener Daten durch das Portal selbst bzw. den Betreiber über das erforderliche Maß hinaus vorsehen,

---

[50] LG Köln, Urteil vom 05.01.2012, Az. 31 O 491/11.

[51] M. w. N.: Weichert in Däubler / Klebe / Wedde / Weichert (Hrsg.), Bundesdatenschutzgesetz Kompaktkommentar, 3. Auflage 2010, § 3 BDSG Rn. 14; Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) vom 27.11.2009, „Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten". https://www.datenschutz.de/aufsicht_privat/ (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

muss jedenfalls gleichwertig und anwendungsfreundlich eine dem Datensparsamkeitsgrundsatz entsprechende Alternative angeboten werden (vgl. 6.1.2 und 6.2.1.2).

6.2.1.2 Einwilligung

Werden Einwilligungen eingeholt, müssen Betroffene gem. § 4a Abs. 1 S. 2 BDSG auf den Zweck der Datenverwendung und gegebenenfalls auf die Folgen einer Verweigerung der Einwilligung hingewiesen werden. Der Betreiber eines Online-Auskunftsportals kann als Diensteanbieter gem. § 13 Abs. 2 TMG Einwilligungen elektronisch einholen, wenn sichergestellt ist, dass Nutzerinnen und Nutzer die Einwilligungen bewusst und eindeutig erteilen, die Einwilligungserklärungen protokolliert werden, jederzeit abrufbar sind und mit Wirkung für die Zukunft widerrufen werden können. Der Betreiber hat die Nutzerinnen und Nutzer gem. § 13 Abs. 3 TMG vor der Erklärung der Einwilligung auf das Widerrufsrecht hinzuweisen. Dieser Hinweis muss jederzeit abrufbar sein.

Einwilligungen sind für das Portal einzuholen, wenn während des Besuchs von Nutzerinnen und Nutzern zur Erstellung eines Auskunftsersuchens personenbezogene Daten gespeichert werden. Dies gilt auch für den Fall, dass die Speicherung nur während des Besuchs (der „Session") stattfindet – etwa um Listen der konkret ausgewählten Stellen, an die ein Auskunftsersuchen gerichtet werden soll, zu erstellen – und nach Beendigung des Besuchs sofort eine Löschung erfolgt. Das Datenschutzrecht kennt keine Erleichterung für kurzfristige Speicherung. Vielmehr wird jede automatisierte Datenverarbeitung als potentielle Gefährdung des Persönlichkeitsrechts angesehen, die einer Rechtfertigung bedarf, um zulässig zu sein. Eine Rechtfertigung der Speicherung kann nicht in der Erforderlichkeit für die Durchführung des Nutzungsverhältnisses, die Erstellung des Auskunftsersuchens, gesehen werden. Denn Auskunftsersuchen können auch auf dem Client des Betroffenen erstellt werden. Insofern besteht keine Erforderlichkeit für die Speicherung der personenbezogenen Daten durch das Portal bzw. den Betreiber. Da bei Fehlen der Erforderlichkeit eine Rechtfertigung nicht ersatzweise über die Abwägung der berechtigten Interessen der verantwortlichen Stelle mit den schutzwürdigen Interessen der betroffenen Person gefunden werden kann[52], ist eine Einwilligung des Betroffenen einzuholen. Zur Gewährleistung der Freiwilligkeit ist gleichwertig und anwendungsfreundlich eine dem Datensparsamkeitsgrundsatz entsprechende Alternative, ohne Speicherung der personenbezogenen Daten durch das Portal bzw. den Betreiber, anzubieten.

Als Zusatzdienst, der durch ein Portal angeboten wird, ist außerdem eine Erinnerungsfunktion denkbar. Der Dienst könnte auf das Ablaufen der im Auskunftsersuchen gestellten Frist oder den Ablauf eines bestimmten Zeitraums, wie etwa eines Jahres, seit Stellen des letzten Auskunftsersuchens, hinweisen. Es ist denkbar, diesen Dienst als E-Mail-Erinnerung durchzuführen. Diese Ausprägung des Dienstes erfordert die Speicherung der E-Mail-Adresse und des Zeitpunkts des Auskunftsersuchens. Die Speicherung durch das Portal bzw. den Betreiber ist allerdings für die Erinnerungsfunktionalität als solche nicht erforderlich. Nutzerinnen und Nutzer des Portals können Erin-

[52] Wedde in Däubler / Klebe / Wedde / Weichert (Hrsg.), Bundesdatenschutzgesetz Kompaktkommentar, 3. Auflage 2010, § 28 Rn. 14, zum Verhältnis der Nummern unter § 28 Abs. 1 BDSG: „Die ergänzenden Tatbestände in den Nr. 2 und 3 können daneben nur außerhalb des Regelungsrahmens von Schuldverhältnissen zur Anwendung kommen".

nerungen über eigene Kalender verwalten. Das Portal könnte hierfür beispielsweise entsprechende Kalenderdateien anbieten. Bietet das Portal eine Erinnerungsfunktion per E-Mail an, ist mangels Erforderlichkeit der Datenspeicherung eine Einwilligung einzuholen. Da diese Funktion nicht zu den essentiellen Diensten gehört, die durch ein Auskunftsportal angeboten werden müssen, um den Kernanforderungen der Nutzerinnen und Nutzer zu entsprechen, muss für diese Funktion keine datensparsame Alternative angeboten werden, um eine freiwillige Einwilligung einholen zu können. Betroffene können ohne große Hürden diese Funktionen mit Hilfe eigener Tools wie Kalendern und Erinnerungsfunktionen erfüllen. In Anbetracht der Zielgruppe des Portals erscheint es jedoch im Sinne einer hohen Glaubwürdigkeit und Attraktivität empfehlenswert, datensparsame und bequeme Hilfsmittel wie passende Kalenderdateien anzubieten.

6.2.1.3 Erhebung von Nutzungsdaten wie IP-Adressen

Der Betreiber eines Online-Auskunftsportals kann Kenntnis über Nutzungsdaten wie IP-Adressen der Nutzerinnen und Nutzer erhalten. Es besteht keine Pflicht zur Speicherung. Webseitenanbieter als Anbieter von Telemedien sind insbesondere nicht zur Speicherung von Nutzungsdaten zur Strafverfolgung verpflichtet. Die nicht zweckgebundene Speicherung der IP-Adressen auf Vorrat ist generell unzulässig (zum Zweckbindungsgrundsatz vgl. 2.1.6).

Eine Erlaubnis zur Speicherung von Nutzungsdaten wie IP-Adressen kann gem. § 15 Abs. 1 TMG bestehen, wenn dies erforderlich ist, um die Erbringung des Dienstes zu ermöglichen. In diesem Fall darf eine Speicherung allerdings nur für die Dauer erfolgen, während der der Dienst erbracht wird.

Zu eigenen Sicherheitszwecken, wie beispielsweise der Detektion von DoS-Angriffen[53], wird von den Datenschutzaufsichtsbehörden im Allgemeinen eine Speicherfrist von maximal sieben Tagen nicht beanstandet. Zulässiger Zweck der Nutzung der IP-Adressen ist in diesem Fall ausschließlich die Sicherstellung des ordnungsgemäßen Betriebs der Datenverarbeitungsanlagen. Es gilt gem. § 31 BDSG eine strenge Zweckbindung.

Gem. § 15 Abs. 3 TMG dürfen Nutzungsprofile (vgl. 6.2.1.4) unter Verwendung von Pseudonymen erstellt werden, sofern der Nutzer dem nicht widerspricht. Nach §§ 15 Abs. 3 S. 2, 13 Abs. 1 TMG hat der Webseitenbetreiber den Nutzer auf sein Widerspruchsrecht hinzuweisen. Analysen des Nutzungsverhaltens anhand personenbezogenen Daten, etwa mit vollständigen IP-Adressen, sind nur mit der bewussten und eindeutigen Einwilligung des Nutzers möglich.

Wird ein kostenpflichtiger Dienst angeboten, dürfen gem. § 15 Abs. 4 S. 1 TMG zu Abrechnungszwecken Nutzungsdaten als Abrechnungsdaten so lange gespeichert werden, wie es für die Zwecke der Abrechnung erforderlich ist (zu Speicherfristen vgl. 6.2.1.7). Die Erforderlichkeit richtet sich nach dem Abrechnungszeitraum und den Einwendungsfristen.

[53] Denial of Service (DoS).

6.2.1.4 Werbung, Optimierung des Dienstes, Statistiken

Für ein Auskunftsportal könnte ein Interesse daran bestehen, das Verhalten der Nutzer zu analysieren, um Statistiken zu erstellen, den Dienst zu optimieren oder die Analysen für Zwecke der Werbung zu nutzen. Rein statistische Erhebungen unter Verwendung von anonymen Daten, d. h. Daten die keinen Personenbezug aufweisen und bei denen ein solcher mit vertretbarem Aufwand auch nicht herstellbar ist (vgl. 2.1.1), sind generell zulässig.

Nutzungsprofile dürfen gem. § 15 Abs. 3 TMG unter Pseudonym für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung des Dienstes erstellt werden. Dies gilt allerdings nur, sofern der Nutzer nicht widerspricht. Der Nutzer ist auf die Erstellung von Nutzungsprofilen und sein Widerspruchsrecht im Rahmen der Datenschutzerklärung auf der Internetseite deutlich hinzuweisen. Widersprüche sind wirksam umzusetzen. Die Nutzungsprofile dürfen nicht mit Daten über die Träger der Pseudonyme zusammengeführt werden. Die Nutzungsdaten sind zu löschen, sobald die Speicherung für die Erstellung des Nutzungsprofils nicht mehr erforderlich ist oder der Nutzer es verlangt.

Zur Erstellung von Nutzungsprofilen ist eine Verwendung der vollständigen IP-Adresse daher ohne eine wirksame Einwilligung der Nutzerin bzw. des Nutzers nicht zulässig. Geolokalisierung, d. h. die Bestimmung des Standorts der Nutzerinnen und Nutzer, darf ohne Einwilligung ebenfalls nicht anhand der vollständigen IP-Adresse erfolgen. IP-Adressen stellen nach der Auffassung der deutschen Datenschutzaufsichtsbehörden keine Pseudonyme im Sinne des TMG dar.[54] Denn IP-Adressen – sowohl statische als in der Regel auch dynamische – sind personenbeziehbare Daten. Sie sind daher vor einer Verwendung so zu kürzen oder zu verändern, dass eine Personenbeziehbarkeit ausgeschlossen ist. Hierfür ist es nicht ausreichend, das letzte Oktett von IPv4-Adressen[55] zu löschen[56], es muss jedenfalls eine Löschung der letzten beiden Oktette erfolgen. Werden IP-Adressen im Rahmen der Anonymisierung durch Pseudonyme ersetzt, ist sicherzustellen, dass eine Reidentifizierung der ursprünglichen IP-Adresse oder eine Identifizierung des Nutzers durch die Zusammenführung mit weiteren Daten ausgeschlossen ist.

Nutzungsprofile werden auch über sog. Cookies erstellt. Cookie-IDs können personenbeziehbare Daten darstellen, wenn die Nutzerin bzw. der Nutzer ggf. auch gemeinsam mit weiteren Daten bestimmbar ist. Personenbezogene Daten stellen jedenfalls dauerhafte Cookies mit einer eindeutigen Benutzerkennung dar.[57] Hinsichtlich des Setzens von Cookies und des Einsatzes vergleichbarerer Technologien sieht Art. 5 Abs. 3 der Datenschutzrichtlinie für elektronische Kommunikations-

---

[54] Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) vom 27.11.2009, „Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten". https://www.datenschutz.de/aufsicht_privat/ (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

[55] Internet Protocol Version 4 (IPv4).

[56] Artikel-29-Datenschutzgruppe, Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen, WP 148, S. 23. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_de.pdf (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

[57] Artikel-29-Datenschutzgruppe, Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen, WP 148, S. 23. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_de.pdf (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

dienste (E-Privacy-Richtlinie, Richtlinie 2002/58/EG, geändert durch die Richtlinie 2009/136/EG[58]) vor, dass grundsätzlich eine Einwilligung des Betroffenen vorliegen muss. Insofern kann die Widerspruchslösung des § 15 Abs. 3 TMG in diesem Zusammenhang keine Anwendung mehr finden. Obwohl die Umsetzungsfrist am 25.05.2011 abgelaufen ist, ist eine Implementierung der geänderten Richtlinie in deutsches Recht bisher nicht erfolgt. Es wird die Auffassung vertreten, das geltende TMG würde die Vorgaben der geänderten Richtlinie bereits berücksichtigen. Für das Setzen von Cookies und den Einsatz vergleichbarer Technologien muss somit grundsätzlich eine Einwilligung der Nutzerin bzw. des Nutzers vorliegen. Ausnahmen können nach Art. 5 Abs. 3 der E-Privacy-Richtlinie vorliegen, wenn der alleinige Zweck des Einsatzes die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz und wenn der Einsatz unbedingt erforderlich ist, damit der Anbieter des Dienstes, der vom Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann. Session-Cookies, die den Nutzer nach dem Login identifizieren und beispielsweise den Login auf jeder weiteren Unterseite entbehrlich machen, fallen regelmäßig unter diese Ausnahme. Nicht unter die Ausnahme fallen zum Beispiel Cookies von Drittanbietern, denn diese Cookies sind für die Nutzung des Dienstes, den Besuch der Webseite, nicht erforderlich. Derartige Cookies werden beispielsweise von sozialen Netzwerken auf Seiten Dritter eingebunden, wie etwa durch den „Gefällt mir"-Button von Facebook.

Gem. § 13 Abs. 7 TMG haben Diensteanbieter Auskünfte nach Maßgabe des § 34 BDSG auch hinsichtlich der zu einem Pseudonym gespeicherten Daten zu erteilen. Werden Nutzungsprofile unter Pseudonymen erhoben, ist demnach ein Verfahren einzurichten, um den Auskunftsanspruch Betroffener zuverlässig erfüllen zu können.

Wird ein Dienstleister damit beauftragt, nach den Weisungen des Auskunftsportals Nutzungsprofile zu erstellen, so handelt es sich in der Regel um Auftragsdatenverarbeitung[59]. Dies setzt voraus, dass der Auftragnehmer keine Eigeninteressen in Zusammenhang mit der Datenverarbeitung verfolgt. Die Vorgaben des § 11 BDSG sind zu beachten, insbesondere ist ein Auftragsdatenverarbeitungsvertrag zu schließen. Auch wenn eine Auftragsdatenverarbeitung vorliegt, sind hinsichtlich der Erstellung der Nutzungsprofile die Vorgaben des TMG zu beachten. Wird der Dienstleister nicht als weisungsabhängiger Auftragsdatenverarbeiter tätig, sondern findet eine Übermittlung an einen Dienstleister als eigenverantwortliche datenverarbeitende Stelle statt, sind Nutzerinnen und Nutzer vor der Übermittlung der Nutzungsdaten, d. h. etwa vor Aufruf des Javascripts oder des Webbugs, über die Übermittlung an den Dritten zu informieren. Es muss die Möglichkeit bestehen, den Dienst auch ohne die Übermittlung an den Dritten zu nutzen.

---

[58] Abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:De:PDF (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

[59] Die Weitergabe von Daten im Auftragsdatenverarbeitungsverhältnis innerhalb des Europäischen Wirtschaftsraums stellt keine Übermittlung dar, § 3 Abs. 4 S. 2 Nr. 3, Abs. 8 S. 3 BDSG, weshalb für die Weitergabe keine Erlaubnis bestehen muss. Für die Speicherung und Nutzung der personenbezogenen Daten muss aber generell eine Rechtfertigung vorliegen.

6.2.1.5 Bewertungsfunktion

Ein Auskunftsportal könnte Nutzerinnen und Nutzern die Möglichkeit bieten, Bewertungen beispielsweise zum Auskunftsverhalten verantwortlicher Stellen wie Unternehmen abzugeben. Dies kann in Form standardisierter Fragen mit einer vordefinierten Antwortskala, aber auch als Freitext erfolgen. Für diesen Dienst ist es grundsätzlich nicht erforderlich, Merkmale zur Identifikation der Nutzerinnen und Nutzer zu erheben. Bewertungen sollten deshalb grundsätzlich anonym abgegeben werden können.

Haftungsrechtlich können für Diensteanbieter gem. § 10 TMG auch im Fall der Speicherung fremder Informationen in zwei Fällen Privilegierungen bestehen. Zum einen kann eine Verantwortlichkeit ausgeschlossen sein, wenn der Diensteanbieter keine Kenntnis von der rechtswidrigen Handlung oder der Information hat und ihm im Falle von Schadensersatzansprüchen auch keine Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird. Zum anderen kann eine Verantwortlichkeit ausgeschlossen sein, wenn er unverzüglich tätig geworden ist, um die Information zu entfernen oder den Zugang zu ihr zu sperren, sobald er Kenntnis erlangt hat. Eine Privilegierung ist ausgeschlossen, wenn die Nutzerin oder der Nutzer, durch die rechtswidrige Inhalte erzeugt werden, dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird. Eine Beaufsichtigung i. S. d. TMG liegt selbst dann nicht vor, wenn eine moderierte Bewertungsfunktion eingesetzt wird.[60] Schaltet der Diensteanbieter Bewertungen nach einer Vorkontrolle frei, nimmt er allerdings Kenntnis von den Inhalten. Es handelt sich nicht um die privilegierte automatische Aufnahme von Inhalten. Diensteanbieter sind gem. § 7 Abs. 2 TMG jedenfalls nicht verpflichtet, die von ihnen gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben davon allerdings unberührt.

Ist die Bewertungsfunktion vollständig anonym ausgestaltet, d. h. werden keine Daten verwendet, die einen Personenbezug aufweisen oder bei denen ein solcher mit vertretbarem Aufwand herstellbar ist (vgl. 2.1.1), ist dies datenschutzrechtlich generell zulässig. Die vollständige Anonymität des Bewertenden kann u. a. zur Folge haben, dass der verantwortlichen Stelle eine Prüfung und Evaluation auf Grundlage einer konkreten Kritik unmöglich ist und eine Bewertung nicht unmittelbar veröffentlicht werden kann, sondern zuvor eine „Unschärfe"-Gruppe[61] gebildet werden muss. Die Anonymität des Bewertenden ist jedenfalls unvereinbar mit einer Erinnerungsfunktion, die per E-Mail einen Link zur Bewertungsfunktion zur Verfügung stellt (vgl. 6.2.1.2).

Es kann ein Interesse daran bestehen, einen objektiv belegten Aussagegehalt der Bewertungen zu erzielen. Hierzu könnten in Bewertungsfunktionen spezifische Regeln implementiert werden. Diese Regeln könnten beispielsweise vorsehen, dass Anfragende eine Bewertung erst nach der gesetzten Antwortfrist und nur innerhalb von zehn Wochen nach Erteilung der Auskunft abgeben dürfen. Für

---

[60] Höfinger / Sieber in Hoeren / Sieber, Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschäftsverkehrs, 32. Ergänzungslieferung, 2012, Teil 18.1 Rn. 94.

[61] Die Bewertungen dürfen erst nach Vorliegen von einer größeren Gruppe aggregiert veröffentlicht werden, damit keine Rückschlüsse möglich sind. Sollte eine verantwortliche Stelle in einem größeren Zeitraum nur ein Auskunftsersuchen und eine Bewertung erhalten haben, so kann die Bewertung einer Person zugeordnet werden.

diesen Zweck müssten etwa der Umstand der Erstellung des konkreten Auskunftsersuchens, der Zeitpunkt der Erstellung, die gesetzte Frist, der Adressat und der Zeitpunkt der Auskunftserteilung verwendet werden. Das Bewertungssystem könnte etwa eindeutige Identifikationsnummern (IDs) jeweils für Auskunftsersuchen und Auskünfte generieren, zu denen die eben beispielhaft dargestellten Kriterien gespeichert werden und anhand derer Verbindungen zwischen Auskunftsersuchen des Betroffenen und angefragter Stelle hergestellt werden. Sie könnten etwa auch als Identifikator für die Freischaltung der Bewertungsfunktion z. B. nach Ablauf der Antwortfrist dienen. Da bei einer solchen Ausgestaltung eines Bewertungssystems jedenfalls ein Personenbezug herstellbar ist, sind die datenschutzrechtlichen Zulässigkeitsanforderungen zu beachten. Da eine Bewertung grundsätzlich auch anonym möglich ist, ist die Personalisierung für diesen Zweck nicht erforderlich. Eine Datenverwendung für diesen Zweck dürfte daher nur mit einer Einwilligung möglich sein (vgl. 6.2.1.2).

Die Bewertungsfunktion ist erst nach Ablauf des gesamten Auskunftsprozesses (Auskunftsersuchen des Betroffenen und Antwort durch die verantwortliche Stelle) von Interesse. Sollte das Portal die Funktion anbieten, per E-Mail eine Erinnerung zu senden, ist – zweckmäßigerweise bei Erstellung des Auskunftsersuchens – eine entsprechende Einwilligung zur Verwendung der E-Mail-Adresse und der weiteren Daten wie Zeitpunkt der Erstellung und Antwortfrist zu dem konkret festgelegten Zweck einzuholen (vgl. 6.2.1.2). Sollte das Auskunftsportal die für Bewertungszwecke erhobenen Daten daneben für andere Zwecke verwenden, ist zuvor ebenfalls eine entsprechende Einwilligung einzuholen.

Natürlich sind auch bei einwilligungsbasierten Lösungen insbesondere die Grundsätze der Transparenz, der Freiwilligkeit und der Datensparsamkeit zu beachten. Dies bedeutet, dass den Nutzerinnen und Nutzern verständlich dargelegt wird, welche Daten zu welchem Zweck verwendet werden. Es ist darauf zu achten, dass die Daten nur für die definierten Zwecke verwendet und gelöscht werden, sobald sie für die Zweckerfüllung nicht mehr erforderlich sind. Für die Gewährleistung der Freiwilligkeit ist daneben eine anonyme Alternative anzubieten.

6.2.1.6 Bezahlsysteme

Es ist denkbar, dass ein Auskunftsportal etwa Informationen oder Dienstleistungen, wie die Übermittlung von Auskunftsersuchen, gegen Entgelt anbietet. Die folgenden Ausführungen betreffen ein Finanzierungsmodell, das durch die Anfragenden getragen wird. Für diesen Fall sind insbesondere die Vorgaben des § 13 Abs. 6 TMG zu beachten. Als Diensteanbieter hat ein Auskunftsportal nicht nur die Nutzung sondern auch die Bezahlung von Telemedien anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Nutzerinnen und Nutzer sind über die Möglichkeit der anonymen oder pseudonymen Bezahlung zu informieren.

Abrechnungsdaten dürfen dabei nur zweckgebunden für die Abrechnung genutzt werden. Sie dürfen höchstens bis zum Ablauf des sechsten Monats nach Versendung der Rechnung gespeichert werden. Eine Verlängerung dieser Frist ist grundsätzlich nur für die Fälle möglich, in denen Forderungen trotz Zahlungsaufforderung nicht beglichen oder Einwendungen dagegen erhoben werden. Eine längere Aufbewahrung von Rechnungsdaten kann nach den Steuergesetzen bzw.

dem Handelsgesetzbuch erforderlich sein, wenn es sich etwa um Handelsbriefe handelt. Je nach Art der Daten sind diese dann in gesperrter Form für maximal sechs bzw. zehn Jahre aufzubewahren (vgl. 2.1.3).

Ein klassisches System zur anonymen Zahlung ist das Angebot, zur Bezahlung Prepaid-Karten zu verwenden. Da dieses inzwischen technisch möglich und in der Regel zumutbar ist, ist dies jedenfalls für die Bezahlung geringer Beträge für Diensteanbieter sogar verpflichtend.[62]

Werden Zahlungsinformationen wie etwa die Kontoverbindung oder Kreditkartendaten erfasst, so ist auf eine Verschlüsselung der Übertragung zu achten (z. B. SSL-Verschlüsselung). Die Daten sind möglichst verschlüsselt aufzubewahren und dürfen außerhalb eines etwaigen Auftragsdatenverarbeitungsverhältnisses nicht weitergegeben werden. Sie sind umgehend zu löschen, wenn sie nicht mehr erforderlich sind, wenn z. B. ein Abonnement ausgelaufen ist und keine Aufbewahrungspflicht besteht.

6.2.1.7 Speicherdauer

Bereichsspezifische Vorschriften wie das TKG, das TMG oder die Abgabenordnung (AO) können spezielle Speicherfristen vorsehen. So sind gem. § 95 Abs. 3 TKG die Bestandsdaten der Teilnehmerin oder des Teilnehmers vom Telekommunikationsdiensteanbieter bei Beendigung das Vertragsverhältnis – sofern eine Speicherung gem. § 95 Abs. 1 TKG überhaupt erforderlich war – mit Ablauf des auf die Beendigung folgenden Kalenderjahres zu löschen. § 15 Abs. 7 S. 1 TMG sieht vor, dass Abrechnungsdaten, die auf Wunsch der Nutzerin oder des Nutzers für die Erstellung eines Einzelnachweises genutzt wurden, spätestens sechs Monate nach Versendung der entsprechenden Rechnung zu löschen sind. Besteht eine Forderung des Diensteanbieters gegen die Nutzerin oder den Nutzer, gegen die Einwendungen erhoben oder die trotz Zahlungsaufforderung nicht beglichen werden, dürfen die Abrechnungsdaten gem. § 15 Abs. 7 S. 2 TMG bis zur Klärung der Angelegenheit gespeichert werden. Für Geschäftsunterlagen wie Buchungsbelege bestehen konkrete Aufbewahrungsfristen von sechs oder zehn Jahren nach § 147 AO. Liegen die tatbestandlichen Voraussetzungen einer Aufbewahrungspflicht vor, sind die entsprechenden Daten gem. § 35 Abs. 3 Nr. 1 BDSG allerdings gesperrt aufzubewahren (vgl. 2.1.3).

Im Übrigen ist die zulässige Speicherdauer abhängig von dem konkreten Speicherzweck. Grundlegend gilt gem. § 35 Abs. 2 S. 2 Nr. 3 BDSG, dass personenbezogene Daten zu löschen sind, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. So ist beispielsweise die Speicherung von Nutzungsdaten wie IP-Adressen grundsätzlich nur so lange zulässig, wie es erforderlich ist, um die Erbringung des Dienstes zu ermöglichen (vgl. 6.2.1.3), in der Regel also nur während der Erbringung des Dienstes.

Werden personenbezoge Daten der Anfragenden zur Erstellung von Auskunftsersuchen, also etwa die Identifikationsdaten und der Adressat, durch den Betreiber des Auskunftsportals gespeichert, ist eine Speicherung über diesen Vorgang hinaus nicht erforderlich (zur grundlegenden Erforderlichkeit einer Speicherung durch den Betreiber eines Auskunftsportals vgl. 6.2.1.2). Nach Erstellung

[62] Vgl. zur Anonymität bei der Verwendung von E-Geld § 25i Kreditwesengesetz (KWG).

des Auskunftsersuchens, der Möglichkeit zum Ausdrucken und Abspeichern müssen die Angaben gelöscht werden. Spätestens hat eine Löschung zu erfolgen, wenn der Browser geschlossen wird. Dies gilt in jedem Fall für die Gewährung unentgeltlicher Leistungen. Andernfalls sind die oben ausgeführten Vorgaben zur Aufbewahrung von Abrechnungsdaten zu beachten.

Datenspeicherungen, etwa für Zwecke eines Erinnerungsservices per E-Mail, können auf der Grundlage einer Einwilligung erfolgen (vgl. 6.2.1.2). Widerrufen Betroffene eine Einwilligung, sind die entsprechenden Daten grundsätzlich unverzüglich zu löschen. Werden Daten über einen Besuch des Portals hinaus gespeichert, ist für den Fall des Widerrufs auch eine zuverlässige Identifikation der Betroffenen vorzusehen, um sicherzustellen, dass nur Berechtigte diesen geltend machen. Die Anforderungen an den Identifikations- und somit praktisch einen Anmeldeprozess sind abhängig von der Bedeutung und der Sensibilität der Daten, die durch den Widerruf gelöscht werden. Im Fall eines Erinnerungsservices per E-Mail dürfte beispielsweise eine Identifikation anhand der E-Mail-Adresse ausreichend sein. In der Bestätigung der Anmeldung könnte zusätzlich ein Link zu einer Abmeldefunktion zur Verfügung gestellt werden.

6.2.1.8 Ort und weitere Vorgaben zur Datenspeicherung

Eine Speicherung von Daten außerhalb des Europäischen Wirtschaftsraums setzt eine Übermittlung in einen Drittstaat voraus. Für diese Übermittlungen sehen §§ 4b, 4c BDSG besondere Voraussetzungen vor, die neben den allgemeinen Zulässigkeitsvoraussetzungen (vgl. 2.1.3) erfüllt sein müssen. So hat eine Übermittlung zu unterbleiben, wenn der Betroffene an dem Ausschluss der Übermittlung ein schutzwürdiges Interesse hat. Dies ist insbesondere der Fall, wenn bei der empfangenden Stelle kein angemessenes Datenschutzniveau gewährleistet ist. Nur für Länder wie Kanada, die Schweiz oder Argentinien hat die Artikel-29-Datenschutzgruppe[63] der Europäischen Kommission ein angemessenes Datenschutzniveau festgestellt. Im Übrigen ist davon auszugehen, dass kein angemessenes Datenschutzniveau herrscht. Es bestehen nur beschränkte Ausnahmen von den restriktiven Vorgaben. Nach § 4c Abs. 1 Nr. 1 BDSG kann etwa eine Ausnahme bestehen, wenn eine Einwilligung des Betroffenen vorliegt. Außerdem kann eine Übermittlung zulässig sein, wenn bestimmte Standardvertragsklauseln ohne Änderungen verwendet werden. Sie enthalten rechtlich durchsetzbare Verpflichtungserklärungen sowie Schutzgarantien für Betroffene. Zudem kann eine Übermittlung zulässig sein, wenn die zuständige Datenschutzaufsichtsbehörde § 4c Abs. 2 BDSG eine Ausnahmegenehmigung erteilt. Hierfür müssen ausreichende Garantien zugunsten der Betroffenen vorgewiesen werden. Diese müssen auf Vertragsklauseln oder verbindlichen Unternehmensregelungen beruhen.

Wird ein Auftragsdatenverarbeiter eingesetzt, stellt eine Weitergabe von Daten an diesen keine Übermittlung an einen Dritten dar. Die Privilegierungen der Auftragsdatenverarbeitung finden allerdings nur für den Fall Anwendung, dass der Dienstleister die Daten im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder innerhalb des Europäischen Wirtschaftsraums verarbeitet. Insofern ist bei der Inanspruchnahme von Cloud-Diensten besondere Vorsicht geboten.

---

[63] http://ec.europa.eu/justice/data-protection/article-29/index_de.htm (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

Auftragsdatenverarbeitung setzt voraus, dass der Dienstleister nach den Weisungen des Auftraggebers tätig wird. Es ist ein schriftlicher Vertrag abzuschließen, der die Vorgaben des § 11 Abs. 2 BDSG berücksichtigt.[64] Insbesondere sind die Dauer des Auftrags und die nach § 9 BDSG durch den Dienstleister zu treffenden technischen und organisatorischen Maßnahmen festzulegen. Außerdem ist beispielsweise vertraglich zu regeln, wie die Berichtigung, Löschung und Sperrung personenbezogener Daten durchzuführen ist und wie bei Beendigung des Vertrags eine Löschung der Daten erfolgen soll. Es empfiehlt sich, für Letzteres ein effektives Nachweisverfahren zu etablieren.

Dienstleister, die Datenverarbeitung im Auftrag vornehmen, sind sorgfältig auszuwählen. Die Auswahl muss nach der Eignung der getroffenen technischen und organisatorischen Maßnahmen erfolgen. Die Einhaltung dieser Maßnahmen hat der Auftraggeber vor Beginn der Datenverarbeitung und regelmäßig während des bestehenden Auftragsverhältnisses zu kontrollieren. Die Kontrollrechte des Auftraggebers sowie die Duldungs- und Mitwirkungspflichten des Auftragnehmers sind in dem Auftragsdatenverarbeitungsvertrag verbindlich zu regeln. Die Ergebnisse der Kontrollen müssen dokumentiert werden.

6.2.2 Datenflüsse

Die Wahrnehmung des Auskunftsrechts erfordert Kommunikation, d. h. die Übermittlung von Daten. Ein Auskunftsportal kann in unterschiedlicher Intensität in diese Datenflüsse eingebunden sein. Das Anbieten spezifischer Dienste bedingt ein entsprechend hohes Maß an Verantwortung. Diese Verantwortung fordert adäquate Sicherungsmaßnahmen.

6.2.2.1 Datenfluss zum Unternehmen

Ein Auskunftsportal wird ein Musteranschreiben für ein Auskunftsersuchen anbieten (vgl. 6.1.3.3). In der „Grundversion" können Anfragende sich die Vorlage ausdrucken und eigenverantwortlich an die angefragte Stelle versenden. Fehler bei der Ausfertigung und Versendung liegen somit ebenfalls in dem Verantwortungsbereich der Anfragenden. Im Falle der Unzustellbarkeit erhält der Anfragende das Auskunftsersuchen an die Absenderadresse zurück.

Das Auskunftsportal könnte als zusätzlichen Service anbieten, die Auskunftsersuchen an die verantwortlichen Stellen zu übermitteln. Auskunftsersuchen durch das Auskunftsportal auszudrucken und postalisch zu versenden, liegt sowohl aus finanziellen als auch aus datenschutzrechtlichen Gründen (vgl. 5.5) fern. Auch ein Versand per Fax oder E-Mail begegnet grundsätzlich Bedenken. Soll ein Übermittlungsdienst angeboten werden, darf das Portal nur als „Bote" tätig werden. Die Übertragung von Signalen über Telekommunikationsnetze stellt gem. § 3 Nr. 24 TKG einen Telekommunikationsdienst dar. Inhalt und nähere Umstände der Kommunikation sind in besonderer Weise durch das Fernmeldegeheimnis nach § 88 TKG geschützt. Es sind entsprechende Strukturen zu entwickeln und nutzen, die in Anbetracht der zentralen Stellung des Portals zudem ausschlie-

[64] BSI, IT-Grundschutz-Kataloge, Baustein B 1.5 Datenschutz, Maßnahme M 7.11 Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten.
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BaustDatenschutz/b01005_pdf.pdf (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

ßen, dass von den Absendern eines Auskunftsersuchens Kenntnis erhalten wird. Auch eine nicht zweckgerichtete, aber theoretisch mögliche Zugriffsmöglichkeit erscheint problematisch und ist daher technisch auszuschließen. Eine Pflicht zur Erhebung und Speicherung besteht für das Auskunftsportal nicht. Nur wer geschäftsmäßig Telekommunikationsdienste erbringt und dabei Rufnummern oder andere Anschlusskennungen vergibt, hat gem. § 111 TKG für die Auskunftsverfahren nach §§ 112, 113 TKG u. a. den Namen und die Anschrift des Anschlussinhabers zu speichern.

Durch einen anonymen Übermittlungsdienst übernimmt das Auskunftsportal eine erhebliche Verantwortung für die Wahrnehmung der Auskunftsrechte der Nutzerinnen und Nutzer. Insbesondere muss die zuverlässige Übermittlung an den richtigen Adressaten sichergestellt sein. Denn schlägt eine Übermittlung fehl, können Nutzerinnen und Nutzer nicht informiert werden. Es droht ein erheblicher Imageschaden, da der eigentliche Zweck des Portals, Unterstützung bei der Wahrnehmung des Auskunftsrechts, in diesem Fall nicht erfüllt wurde. Die Risiken können eingedämmt werden, indem sichere Kommunikationskanäle zu teilnehmenden Organisationen aufgebaut werden. Mit diesen Stellen ist vertraglich zu vereinbaren (vgl. 6.3.6), dass jederzeit die technische Empfangsbereitschaft gewährleistet sein muss und andernfalls vorab, bei Unvorhersehbarkeit unverzüglich, eine Meldung mit einer zeitlichen Bestimmung der Einschränkung erfolgt. Es sollte vereinbart werden, dass hinsichtlich unvorhersehbarer Ausfälle Fehlerberichte zu erstellen und dem Portal vorzulegen sind, aus denen Abhilfe- und Verbesserungsmaßnahmen für die Zukunft sowie ein Zeitplan zur Umsetzung ersichtlich sind. Nutzerinnen und Nutzern sollte eine Möglichkeit eingeräumt werden, Unregelmäßigkeiten bei der Abwicklung von Auskunftsersuchen, die über das Portal übermittelt worden sind, zu melden. Die Meldung sollte sowohl der angefragten Stelle als auch dem Portal zugehen. Im Fall der Einschränkung der Empfangsbereitschaft ist technisch sicherzustellen, dass Nutzerinnen und Nutzern der Service für den angegebenen Zeitraum bzw. bis auf Weiteres für die betreffende Organisation bzw. das Unternehmen nicht angeboten wird. Es ist dann auf die Grundversion der Übermittlung in Eigenverantwortung zu verweisen.

Wird ein Übermittlungsdienst angeboten, muss berücksichtigt werden, dass eine ungewöhnliche Konstellation eines Kommunikationsverhältnisses vorliegt. In der Regel werden Anfragen an den Absender beantwortet. Ist ein Dritter wie ein Auskunftsportal eingebunden, muss aus dem Auskunftsersuchen grundsätzlich – vorbehaltlich anderer durch den Anfragenden ausdrücklich gewünschter Dienste – hervorgehen, dass die Auskunft direkt an den Anfragenden zu erfolgen hat.

6.2.2.2 Datenfluss zum Verbraucher

Verantwortliche Stellen wie Unternehmen könnten ein wirtschaftliches Interesse daran haben, im Verhältnis zum Postversand kostengünstigere elektronische Übermittlungswege zum Anfragenden nutzen zu können. Anfragende haben ein Interesse daran, Auskunftsersuchen in praktischer informationeller Selbstbestimmung durchzuführen. Ein Portal könnte dazu einen Beitrag leisten, indem es Möglichkeiten des elektronischen Identitätsnachweises und des Einsatzes von Verschlüsselungstechnologien erläutert und insbesondere deren praktische Handhabung verbrauchergerecht darstellt.

Eine Einbindung eines Auskunftsportals – wie auch jedes anderen Dritten – bei der Übermittlung der Auskunft an den Anfragenden ist datenschutzrechtlich kritisch zu betrachten (vgl. 5.5). U. a. aufgrund der sensiblen, verifizierten Informationen, die übermittelt werden. Werden derartige Telekommunikationsdienste angeboten, sind der Inhalt und die näheren Umstände der Kommunikation jedenfalls durch das Fernmeldegeheimnis nach § 88 TKG – auch und gerade gegenüber dem Telekommunikationsdiensteanbieter – geschützt.

Zudem ergibt sich bei der Einbindung des Portals die Problematik der zuverlässigen Authentisierung des tatsächlich zum Erhalt der Auskunft Berechtigten (vgl. 2.3.2). Nur an diesen darf eine Auskunft erteilt werden (vgl. 4.3), was gewöhnlich über einen Abgleich der Absenderadresse mit dem vorhandenen Datenbestand und einer Versendung der Auskunft an diese Anschrift sichergestellt ist. Zwar ist denkbar, mit zunehmender Verbreitung des nPA dessen eID-Funktion für einen Identitätsnachweis einzusetzen. Die Funktion ist gerade auch im Internet sowie gegenüber privaten Stellen nutzbar. Auslesende Stellen benötigen allerdings gem. § 18 Abs. 4 PAuswG ein Berechtigungszertifikat. Die Vergabestelle für Berechtigungszertifikate (VfB) prüft gem. § 21 PAuswG auf Antrag, ob ein Berechtigungszertifikat erteilt werden kann und ggf. welche der zwölf Datenfelder des nPA ausgelesen werden dürfen. Es erscheint äußerst fraglich, ob die Einrichtung eines „Identitätsnachweis-Dienstes“ durch das Portal, der angefragten Stellen den Erwerb eines eigenen Berechtigungszertifikats erspart, zulässig wäre. Die datenschutzrechtliche Problematik der zentralen Stellung des Portals (vgl. 5.5) würde in besonderer Weise hervortreten. Eine Erhebung von Identifikationsdaten ist nur durch die angefragte Stelle erforderlich. Entsprechende Bedenken ergeben sich für den Einsatz der Funktion De-Ident (Möglichkeit zur Identitätsfeststellung im Rahmen der De-Mail-Dienste) im Verhältnis zwischen Anfragenden und Auskunftsportal zur Erteilung einer Auskunft.

6.2.3 Technische und organisatorische Anforderungen

Bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist gem. § 9 BDSG im erforderlichen Umfang technisch und organisatorisch zu gewährleisten, dass die datenschutzrechtlichen Vorgaben eingehalten werden. Erforderlich sind technische und organisatorische Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist nach Anlage zu § 9 S. 1 BDSG die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speiche-

rung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),

4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Maßnahmen zur Zugangs-, Zugriffs- und Weitergabekontrolle sind insbesondere die Verwendung von Verschlüsselungsverfahren, die dem Stand der Technik entsprechen.

Gem. § 13 Abs. 4 TMG haben Anbieter von Telemedien und somit ein Online-Auskunftsportal durch technische und organisatorische Vorkehrungen sicherzustellen, dass

1. der Nutzer die Nutzung des Dienstes jederzeit beenden kann,
2. die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht oder in den Fällen des § 13 Abs. 4 S. 2 TMG gesperrt werden,
3. der Nutzer Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann,
4. die personenbezogenen Daten über die Nutzung verschiedener Telemedien durch denselben Nutzer getrennt verwendet werden können,
5. Daten nach § 15 Abs. 2 TMG nur für Abrechnungszwecke zusammengeführt werden können und
6. Nutzungsprofile nach § 15 Abs. 3 TMG nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden können.

Gem. § 13 Abs. 4 S. 2 TMG tritt an die Stelle der Löschung nach § 13 Abs. 4 S. 1 Nr. 2 TMG eine Sperrung, soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen.

6.2.3.1 Test und Freigabe

Test und Freigabe sollen sicherstellen, dass die fachgerechte Installation und Konfiguration eines Systems vorgenommen und anschließend die Verantwortung für den Betrieb von der verantwortlichen Stelle übernommen wird. Tests müssen nach Testplänen durchgeführt werden, die die Anforderungen vorgeben, die durch das System zu erfüllen sind.[65] Der Datenschutzbeauftragte eines Auskunftsportals ist gem. § 4g Abs. 1 S. 4 Nr. 1 BDSG rechtzeitig über Vorhaben der automatisierten Datenverarbeitung und somit auch über die Durchführung von Test und Freigabe zu informieren.[66] Ihm ist Gelegenheit zu geben, Einfluss auf die Durchführung des Verfahrens zu nehmen und beispielsweise den Testplan zu ergänzen.

Für Testzwecke dürfen grundsätzlich nur Testdaten verwendet werden. Das heißt, dass in der Regel keine personenbezogenen Echtdaten beispielsweise von Auskunftssuchenden verwendet werden dürfen.

Die Voraussetzungen und insbesondere die Zuständigkeiten für eine Freigabe müssen genau festgelegt sein. Einer Freigabe muss in jedem Fall eine datenschutzrechtliche Prüfung des getesteten Verfahrens vorausgegangen sein.

Die Maßnahmen und Ergebnisse der Tests sowie die Freigaben müssen revisionssicher dokumentiert werden (vgl. 6.2.3.2).

6.2.3.2 Verfahrensdokumentation

Dokumentation dient dem Zweck, Prüfbarkeit beispielsweise für den eigenen Datenschutzbeauftragten oder die Aufsichtsbehörde herzustellen. Es muss dargelegt werden können, dass gem. § 9 BDSG ausreichende technische und organisatorische Maßnahmen getroffen worden sind, um die Ausführung der datenschutzrechtlichen Vorschriften zu gewährleisten. Eine umfassende, verständliche Dokumentation dient aber auch dem Eigeninteresse der Organisation, die Funktionsfähigkeit der eingesetzten Verfahren kontrollieren und gewährleisten zu können. Die Dokumentation soll für sachkundige Personen in angemessener Zeit nachvollziehbar sein. Sie besteht regelmäßig aus verschiedenen Komponenten, die aufeinander Bezug nehmen.

In einer Dokumentation der eingesetzten Informationstechnik sind die eingesetzten IT-Geräte und die eingesetzten Programme zu dokumentieren. In einem Netzplan sind die physikalischen und logischen Verbindungen zwischen Geräten darzustellen.

In einer Dokumentation der getroffenen Sicherheitsmaßnahmen sind die technischen und organisatorischen Maßnahmen zur Gewährleistung der Ausführung der datenschutzrechtlichen Vorschriften zu erfassen. So wird dies beispielsweise in der Regel eine Dokumentation der eingesetz-

---

[65] BSI, IT-Grundschutz-Kataloge, Baustein B 1.5 Datenschutz, Maßnahme M 7.9 Datenschutzrechtliche Freigabe. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BaustDatenschutz/b01005_pdf.pdf (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

[66] BSI, IT-Grundschutz-Kataloge, Baustein B 1.5 Datenschutz, Maßnahme M 7.13 Dokumentation der datenschutzrechtlichen Zulässigkeit.
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BaustDatenschutz/b01005_pdf.pdf (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

ten Verschlüsselungs- und Protokollierungsmechanismen umfassen. Außerdem müssen beispielsweise die Maßnahmen zur Umsetzung des Datensparsamkeitsgrundsatzes dokumentiert werden. Die Überprüfung der Erforderlichkeit und Angemessenheit der getroffenen Sicherheitsmaßnahmen ist in Form einer Risikoanalyse zu dokumentieren.

Zu jedem eingesetzten Verfahren muss ein Verfahrensverzeichnis bestehen.[67] Aus Art. 18 Abs. 1 EG-DSRL geht hervor, dass unter einem Verfahren eine Verarbeitung oder eine Mehrzahl von Verarbeitungen zur Realisierung einer oder mehrerer verbundener Zweckbestimmungen zu verstehen ist. Der Begriff „automatisiertes Verfahren" ist beispielsweise in § 2 Datenschutzverordnung Schleswig-Holstein definiert als Arbeitsabläufe mit Hilfe von informationstechnischen Geräten, Programmen und automatisierten Dateien. Das Verfahrensverzeichnis muss jedenfalls die Angaben nach § 4e BDSG enthalten. Zudem muss ein Verzeichnis über die zum Zugriff berechtigten Personen bestehen.[68] Zu jedem Verfahren soll die Durchführung von Test und Freigabe (vgl. 6.2.3.1) dokumentiert werden.

Werden Datenverarbeitungen ausgelagert und durch Auftragnehmer wie Provider durchgeführt, sind die Aufträge schriftlich zu erteilen und müssen den in § 11 Abs. 2 BDSG vorgegebenen Mindestregelungsgehalt umfassen. Insbesondere müssen die nach § 9 BDSG zu treffenden Maßnahmen vorgegeben werden. Deren Einhaltung muss vor Beginn der Datenverarbeitung und im Folgenden regelmäßig überprüft werden. Die Ergebnisse müssen dokumentiert werden.

6.2.3.3 Protokollierung

Die Vorgaben des BDSG implizieren Kontrollziele wie Eingabe- oder Verantwortlichkeitskontrolle. Insbesondere die technisch-organisatorischen Vorgaben der Anlage zu § 9 BDSG setzen Nachweismöglichkeit voraus. Diese Nachweise erfolgen in der Regel anhand von Protokolldaten. Sie müssen darüber Auskunft geben können, wer wann welche personenbezogenen Daten in welcher Weise und zu welchem Zweck verarbeitet hat.[69]

Protokollierungsverfahren[70] sind nach den Grundsätzen der Datensparsamkeit (vgl. 2.1.4) und der Erforderlichkeit (vgl. 2.1.5) zu gestalten. Da Protokolldaten naturgemäß dennoch sehr weitgehende Informationen beispielsweise zu dem Abrufverhalten der Nutzer enthalten, unterliegen sie gem.

---

67 BSI, IT-Grundschutz-Kataloge, Baustein B 1.5 Datenschutz, Maßnahme M 7.8 Führung von Verfahrensverzeichnissen und Erfüllung der Meldepflichten bei der Verarbeitung personenbezogener Daten. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BaustDatenschutz/b01005_pdf.pdf (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

68 BSI, IT-Grundschutz-Kataloge, Maßnahmenkatalog M 2 Organisation, Maßnahme M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02031.html (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

69 Orientierungshilfe „Protokollierung", herausgegeben vom Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Stand 2. November 2009, S. 3.

70 BSI, IT-Grundschutz-Kataloge, Maßnahmenkatalog M 2 Organisation, Maßnahme M 2.110 Datenschutzaspekte bei der Protokollierung. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02110.html (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

§ 31 BDSG einer strengen Zweckbindung. Sie dürfen ausschließlich für die Zwecke verwendet werden, für die sie erhoben wurden, also insbesondere der Datenschutzkontrolle und der Sicherstellung des ordnungsgemäßen Betriebs des Systems. Zu jedem Protokolldatum muss die Aufbewahrungsdauer festgelegt sein. Soweit nicht spezialgesetzliche Aufbewahrungspflichten bestehen, richten sich diese nach den allgemeinen datenschutzrechtlichen Vorgaben zur Löschung. In der Regel dürfen Daten nur so lange vorgehalten werden, wie es zur Erfüllung des vorgesehenen Zwecks erforderlich ist.

Es muss ein Protokollierungskonzept vorliegen, das die genannten Punkte berücksichtigt und Zugriffs- und Auswertungsberechtigungen für die Protokolldaten festlegt. Empfehlenswert ist bei der Konzeption die Orientierung an den üblichen Lebenszyklusmodellen. Typische Phasen sind:

- Erzeugen (Festlegung von Art und Umfang der Protokollierung),
- Übertragen (ggf. Sicherung von Übertragungen, falls externe Protokollierungssysteme wie zentrale Syslog-Server verwendet werden),
- Speichern (Festlegung, ob eine Sofortauswertung möglich ist oder eine Speicherung erfolgen soll; Zugriffsschutz und Backup für Kontrolldaten, Manipulationsschutz),
- Auswerten (Beachtung von Mitbestimmungsrechten, Erstellung typischer Auswertungsszenarien),
- Löschen (Festlegung von Aufbewahrungsfristen, rückstandsfreie Löschung).

Administrative Tätigkeiten können besonders weitreichende Auswirkungen auf Systeme haben. Die Vornahme derartiger Tätigkeiten muss daher einer besonderen Kontrolle unterliegen. Insbesondere die Installation, Modifikation und Konfiguration von Hard- und Software müssen als grundlegende Voraussetzungen für die Nachvollziehbarkeit der Funktionsweise und der Sicherheit des Systems protokolliert werden. Es muss ausgeschlossen sein, dass Änderungen an Protokolldaten vorgenommen werden können.

Die Nutzung von Systemen muss insoweit protokolliert werden, als es zum Nachweis einer rechtmäßigen Datenverwendung erforderlich ist. In der Regel werden die Vorgänge der Authentifizierung und Autorisierung, des lesenden Zugriffs, des schreibenden Zugriffs (Dateneingabe und -veränderung), der Datenübermittlung und der Datenlöschung zu protokollieren sein.

6.2.3.4 Netzsicherheit

Ein Online-Auskunftsportal wird über einen Webserver bereitgestellt. Ein solcher ist ein öffentlich zugängliches System, das an ein öffentliches Netz wie beispielsweise das Internet angebunden ist. Solche Systeme können nicht nur direkt angegriffen werden. Es können über das Netz von beliebigen Orten Angriffe initiiert werden. Die Gefährdungslage ist somit ungleich höher als bei Systemen, die keine Verbindung zum Internet vorhalten. Es müssen dem Sicherheitsbedarf der auf dem System gespeicherten Daten und der installierten Anwendungen entsprechende Maßnahmen getroffen werden. Insbesondere die Installation und Konfiguration dieses Systems und seiner Netzumgebung sind sorgfältig durchzuführen. Ausführliche Hinweise hierzu enthält Baustein B 5.4

„Webserver“[71] der IT-Grundschutz-Kataloge des BSI, der einzelne Gefährdungslagen für den Betrieb eines Webservers identifiziert und daraus Maßnahmenempfehlungen für die „Planung und Konzeption“, „Beschaffung“, „Umsetzung“, „Betrieb“ und „Notfallvorsorge“ ableitet.

Ein zentraler Aspekt des sicheren Betriebs eines Webservers ist die Regelung der Zugriffe auf das System. Um nur erwünschte Zugriffe auf den Webserver zuzulassen, muss die Kommunikation technisch auf das erforderliche Maß eingeschränkt werden. Dies erfolgt in der Regel anhand von Firewalls. Detaillierte Ausführungen hierzu enthält B 3.301 „Sicherheitsgateway (Firewall)“[72] der IT-Grundschutz-Kataloge des BSI.

6.2.3.5 Webhosting

Wird durch ein Auskunftsportal das Webhosting an einen Provider ausgelagert, könnte es sich um eine Auftragsdatenverarbeitung handeln. Dies setzt voraus, dass der Provider nach Vorgaben des Auftraggebers tätig wird. Liegt eine Auftragsdatenverarbeitung vor, stellt eine Weitergabe von Daten an den Provider keine Übermittlung an einen Dritten dar. Allerdings gilt dies nur für den Fall, dass der Provider die Daten im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder innerhalb des Europäischen Wirtschaftsraums verarbeitet. Außerhalb dieses Raums finden die Privilegierungen der Auftragsdatenverarbeitung keine Anwendung. Insofern ist besondere Aufmerksamkeit hinsichtlich der Inanspruchnahme von Cloud-Dienstleistungen aufzuwenden.

Für die Festlegung der technisch-organisatorische Maßnahmen im Zusammenhang mit dem Auslagern eines Betriebs auf einen externen Dienstleister gibt der Baustein B 1.11 „Outsourcing“[73] der IT-Grundschutz-Kataloge des BSI wesentliche Hinweise.

6.2.3.6 Datenschutzmanagement

Die Implementierung und Sicherstellung des notwendigen und angemessenen Datenschutzniveaus ist, wie viele andere Aspekte innerhalb einer Organisation, kein einmaliges Vorhaben. Vielmehr ist es eine Daueraufgabe, die Organisationen vorzugsweise mit Hilfe von strukturierten Prozessen bearbeiten. Aus den gesetzlichen Vorschriften für behördliche und betriebliche Datenschutzbeauftragte[74] ergeben sich erste Ansatzpunkte für ein Datenschutzmanagement. Hinzu

---

[71] BSI, IT-Grundschutz-Kataloge, Baustein B 5.4 Webserver. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b05/b05004.html (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

[72] BSI, IT-Grundschutz-Kataloge, Baustein B 3.301 Sicherheitsgateway (Firewall). https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b03/b03301.html (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

[73] BSI, IT-Grundschutz-Kataloge, Baustein B 1.11 Outsourcing. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b01/b01011.html (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

[74] Etwa § 4g BDSG: Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin. [...] Er hat insbesondere [...] die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten, [...].

kommen organisatorische Aspekte, die sicherstellen, dass die Aufgaben entsprechend den datenschutzrechtlichen Vorgaben und mit dauerhaft hoher Qualität erfüllt werden.

Ein Datenschutzmanagementsystem gewährleistet dies durch eine den einzelnen Verfahren übergeordnete Organisationsstruktur. Veränderungen, beispielsweise technischer und rechtlicher Umstände, werden zentral erfasst und gezielt in die davon betroffenen Verfahren eingesteuert. Hierfür muss sichergestellt werden, dass interne und externe relevante Änderungen sowie Funktionsstörungen innerhalb bestehender Verfahren zuverlässig registriert werden. Vor allem muss organisatorisch gewährleistet sein, dass adäquate Reaktionen erfolgen bzw. Reaktionsketten eingeleitet werden. Zuständigkeiten und Berichtswege sind vorab konkret festzulegen.

Voraussetzung für ein effektives Datenschutzmanagementsystem ist eine genaue Kenntnis der bestehenden und geplanten Datenverarbeitungsverfahren.[75] So muss beispielsweise konkret bekannt sein, an welchen Stellen, zu denen etwa auch Zwischenspeicher-, Archiv- oder Backup-Dateien zählen können, personenbezogene Daten von der verantwortlichen Stelle erhoben und gespeichert werde. Nur so können etwa Löschvorgaben[76] vollständig umgesetzt werden.

Der Aufbau eines Datenschutzmanagementsystems kann sich beispielsweise an den IT-Grundschutz-Katalogen des BSI (Maßnahme M 7.1 „Datenschutzmanagement" des Bausteins „Datenschutz")[77] orientieren. Dieses Konzept sieht einen zyklischen Datenschutzprozess vor, der aus den drei Schritten „Erstellung des Datenschutzkonzeptes und Soll-Ist-Abgleich", „Umsetzung fehlender Maßnahmen" und „Aufrechterhaltung des Datenschutzes im laufenden Betrieb" besteht.

6.3 Vertrauenswürdigkeit des Portals

Ein Auskunftsportal weckt bei den verschiedenen betroffenen Interessengruppen bestimmte Erwartungen. Zu den verschiedenen Interessengruppen zählen Verbraucherinnen und Verbraucher sowie Verbraucherschutzverbände, Unternehmen und Unternehmerverbände sowie Datenschutzaussichtsbehörden und Datenschutzorganisationen. Die Verbände und Organisationen werden dabei im Folgenden als Vertreter der entsprechenden Interessen einbezogen. Die Interessen können sich unterscheiden, evtl. sogar gegensätzlich darstellen.

- Verbraucherinnen und Verbraucher erwarten, dass ein Auskunftsportal sie umfassend und objektiv über ihr Auskunftsrecht informiert und bei der Stellung eines Auskunftsersuchens effektiv unterstützt. Von einem Portal, das sich für Datenschutzbetroffenenrechte engagiert, wird keine Ausgestaltung erwartet, die Unternehmensinteressen einseitig berücksichtigt.

---

[75] Gem. § 4g Abs. 2 BDSG ist dem betrieblichen Datenschutzbeauftragten eine Übersicht zu den Verfahren automatisierter Datenverarbeitung – zum Verfahrensverzeichnis vgl. 2.1.9 – zur Verfügung zu stellen.

[76] Vgl. etwa zur Erstellung eines Löschkonzepts: Deutsches Institut für Normung e.V. (DIN), Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten. http://www.secorvo.de/publikationen/din-leitlinie-loeschkonzept-hammer-schuler-2012.pdf (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

[77] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BaustDatenschutz/b01005_pdf.pdf (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

- Unternehmen werden evtl. erwarten, sich innerhalb eines solchen Portals möglichst positiv präsentieren zu können. Hinsichtlich der Ausgestaltung des Portals könnte die Erwartung bestehen, dass für das Unternehmensimage und die Arbeitsbelastung möglicherweise nachteilige Angebote oder Funktionen nicht angeboten werden.
- Datenschutzaufsichtsbehörden erwarten, dass die gesetzlichen Vorgaben im Interesse des Betroffenen angewendet und insbesondere der Datensparsamkeitsgrundsatz berücksichtigt wird. Eine Realisierung mit innovativen datenschutzfreundlichen Ausgestaltungsmöglichkeiten wird begrüßt. Eine zuverlässige und sachliche Information und Unterstützung der Betroffenen bei der Wahrnehmung des Auskunftsrechts als essentielles Datenschutzrecht wäre zu begrüßen. Ebenso wäre eine objektive Information und ggf. Unterstützung der Unternehmen als verantwortliche Stellen begrüßenswert.

Trägt eine der Interessengruppen in erheblichem Umfang zur Finanzierung des Auskunftsportals bei, wird dies regelmäßig im Ausgestaltungsprozess bei der Berücksichtigung der Interessen Niederschlag finden. Eine einseitige Berücksichtigung würde zum Nachteil der übrigen Interessengruppen gereichen.

Für die Vertrauenswürdigkeit des Portals ist es entscheidend, dass es in Unabhängigkeit tätig wird. Dies erfordert vor allem, dass Entscheidungen insbesondere hinsichtlich der Ausgestaltung unabhängig, d. h. frei von den Weisungen getroffen werden.

Je nach Ausgestaltung des Portals und den Zielen, denen es sich verschreibt, erhält es von den Interessengruppen entsprechendes Vertrauen bzw. Unterstützung. Es ist entscheidend, die für die Akzeptanz des Portals wesentlichen Erwartungen zu erkennen und diese bei der Ausgestaltung des Portals ausgewogen zu berücksichtigen. Andernfalls ist zweifelhaft, ob sich ein Auskunftsportal nachhaltig etablieren kann.

6.3.1 Vorbildfunktion des Portals

An ein Auskunftsportal werden die verschiedenen Interessengruppen spezifische Erwartungen stellen. Insbesondere dürfte wegen des Engagements des Portals in grund- und verbraucherrechtlichen Fragen ein entsprechend vorbildliches nutzer- und verbraucherfreundliches Agieren erwartet werden. Von einem Portal, das sich für Datenschutzrechte engagiert, wird erwartet, dass es selbst Datenschutzvorgaben in vorbildlicher Weise umsetzt und über das gesetzliche Mindestmaß hinaus besonders datenschutzfreundliche Lösungen forciert. Ein Mehrwert kann für Verbraucherinnen und Verbraucher entstehen, wenn etwa die Benutzerfreundlichkeit derartiger Lösungen und die Tauglichkeit für den Massenbetrieb vorangetrieben wird. Insofern kann ein Portal Vorbild und Orientierungsgröße für Unternehmen und andere Webseitenbetreiber sein.

6.3.2 Rechtsform des Portals

Ein bedeutender Aspekt der Vertrauenswürdigkeit des Portals ist die Wahl der Rechtsform des Portals. Denn dies ist maßgeblich dafür, wer hinsichtlich des Betriebs und der Ausgestaltung des Portals entscheidungsbefugt ist. Zudem werden bestimmte Rechtsformen wie Gesellschaften mit be-

schränkter Haftung (GmbH) oder Aktiengesellschaften (AG) von der Öffentlichkeit als primär gewinnorientiert angesehen. Insofern hätte die Wahl einer solchen Rechtsform wohl negative Auswirkungen auf das Image und die Vertrauenswürdigkeit des Portals.

Natürlich könnte durch Maßnahmen wie die Installation eines Beirats einem möglichen Vertrauensverlust entgegengewirkt werden. Dabei dürfte zwar relevant sein, wie ein solcher zusammengesetzt ist und welche Befugnisse ihm eingeräumt werden. Ein Beirat nimmt jedoch regelmäßig nur eine beratende Funktion ein und verfügt nicht über Entscheidungsbefugnisse. Daher bestehen Zweifel, ob diese Maßnahme ausreichend wäre. Denn die grundlegenden und richtungsweisenden Entscheidungen treffen die Organe der Gesellschaft wie etwa im Falle einer GmbH die Gesellschafter. Befugnisse und Zusammensetzung des Beirats, nicht zuletzt seine Existenz, werden durch die Organe der Gesellschaft bestimmt.

Eine andere Möglichkeit, die Vertrauenswürdigkeit des Portals zu unterstützen, wäre, die Form einer Non-Profit-Organisation (NPO), beispielsweise einer Stiftung oder eines Idealvereins, bzw. einer gemeinnützigen Organisation zu wählen. Aber eine solche Organisationsform ist nicht per se eine vertrauenswürdige Alternative. Es ist entscheidend, wie die Ausgestaltung erfolgt, also insbesondere, wer Entscheidungsträger ist, welche Entscheidungen getroffen werden und wie finanzielle Mittel eingesetzt werden. Eine NPO, die propagiert, sich für Datenschutz- und Verbraucherrechte zu engagieren, aber überdurchschnittlich gut dotierte Aufträge an Unternehmen vergibt, die etwa „Partner" des Portals oder in sonstiger Form beteiligte sind, könnte die Vertrauenswürdigkeit des Portals beschädigen. Insofern sind auch bei dieser Organisationsform vertrauenswürdige Konzepte sowie verbindliche Regelungen und Strukturen für die Öffentlichkeit transparent und kontrollfähig darzustellen.

6.3.3 Finanzierung

Die Finanzierung eines vertrauenswürdigen und nachhaltigen Auskunftsportals stellt eine Herausforderung dar. Es besteht im Sinne des Datenschutzes ein Interesse daran, das Auskunftsrecht als Datenschutzbetroffenenrecht zu stärken. Der Einfluss bestimmter Gruppen mit entgegenstehenden Interessen darf nicht dazu führen, dass diese Interessen die Ausgestaltung des Portals bestimmen. Das gilt insbesondere auch für den Fall, dass diese Interessengruppen einen erheblichen finanziellen Beitrag zu dem Betrieb des Portals leisten.

Ein ausgewogenes Finanzierungskonzept könnte bei den hauptsächlichen Nutznießern des Portals ansetzen. Dazu zählen Nutzerinnen und Nutzer sowie Organisationen wie Unternehmen. Inwieweit erstere bereit sind, für die erleichterte Wahrnehmung gesetzlich garantierter Rechte einen Beitrag zu zahlen, wäre zu prüfen.

Organisationen wie Unternehmen können entscheidend davon profitieren, dass sie sich selbst, ihre Datenschutzgrundsätze sowie weitere Inhalte im Portal präsentieren können. Hierdurch können gezielt Fragen vorweggenommen werden, die sonst zu einem Auskunftsersuchen und Arbeitsaufwand in der Organisation führen würden. Wird ein Auskunftsersuchen mit Hilfe des Portal erstellt, erhält die Organisation eindeutig formulierte Auskunftsersuchen und kann diese effektiv in ihre Prozesse integrieren (vgl. 5.2). Für diese Leistungen könnten Organisationen wie Unternehmen

bereit sein, einen „Teilnahmebeitrag" zu zahlen. Der Beitrag sollte dabei stets in einem angemessenen Verhältnis zu der erhaltenen Leistung stehen, damit keine Gründe für den Verdacht der Einflussnahme auf das Portal und seine Ausrichtung bestehen.

Weitere Finanzierungsmöglichkeiten sind auf ihre Realisierbarkeit und Dauerhaftigkeit zu prüfen.

6.3.4 Interne Kontrollsysteme

Für die Vertrauenswürdigkeit des Portals spielen neben der geeigneten Rechtsform und dem geeigneten Finanzierungsmodell auch die Integration leistungsfähiger Kontrollsysteme in die Aufbau- und Ablauforganisation eine entscheidende Rolle. Dadurch wird sichergestellt, dass die langfristige Ausrichtung des Portals und die kurzfristigen Entscheidungen im „Tagesgeschäft" geprüft und kritisch hinterfragt werden. Dies ist erforderlich, da ein Portal im Fokus der Öffentlichkeit stehen wird und sich an hohen Maßstäben messen lassen muss.

Eine Maßnahme innerhalb eines solchen Kontrollsystems könnte die Bestellung eines starken betrieblichen Datenschutzbeauftragten im Rahmen eines umfassenden Datenschutzmanagements darstellen. Die Stärke zeichnet sich dabei durch direkte Berichtswege zu den leitenden Organen und ein tatsächlich weisungsfreies Tätigwerden aus.

Diese unabhängige Kontrollinstanz könnte von Transparenz- bzw. Öffentlichkeitsmaßnahmen flankiert werden. Das Portal könnte sich etwa einer öffentlichen Diskussion über seine Ausgestaltung und die Organisationsform stellen. Der Transparenzgedanke bezieht sich hierbei auf das Portal, seinen Umgang mit den verschiedenen Interessen sowie sein Leistungsangebot bzw. die technische Umsetzung.

Ein Beirat (vgl. 6.3.2) könnte als zusätzliches Kontrollinstrument agieren. Der positive Einfluss auf die Vertrauenswürdigkeit des Portals hängt aber von dessen konkreten Aufgaben, der Zusammensetzung und den eingeräumten Befugnissen ab. Im Gegensatz zum betrieblichen Datenschutzbeauftragten[78] sind Bestellung und Aufgaben eines Beirats nicht gesetzlich geregelt.

6.3.5 Zertifizierung

Die Zertifizierung eines Auskunftsportals trägt zum Transparenzgedanken bei. Sie kann zu einer positiven Öffentlichkeitswirkung beitragen. Es sollte deshalb besondere Aufmerksamkeit auf die Auswahl des Zertifizierungskonzeptes, den Aussagegehalt des verliehenen Siegel und der Seriosität des Anbieters gelegt werden. Bei den verschiedenen Zertifizierungskonzepten und Anbietern von Zertifizierungen bestehen große Qualitätsunterschiede. Die Bandbreite reicht von sehr geringen Anforderungen, um das angestrebte Gütesiegel zu erreichen, bis hin zu sehr umfangreichen Konzepten, die höchste Anforderungen an die Siegelvergabe stellen. Sollte ein Zertifizierungskonzept bzw. das dazugehörige Gütesiegel negativ in der Öffentlichkeit auffallen, so wirkt sich dies in der Regel auf alle Träger dieses Gütesiegels nachteilig aus und sie müssen sich ggf. der negativen Presse stellen. Von Gütesiegeln mit besonders hohen Qualitätsanforderungen und der dazugehö-

[78] Vgl. für den betrieblichen Datenschutzbeauftragten §§ 4f, 4g BDSG.

rigen positiven Außendarstellung kann im Gegenzug besonders profitiert werden. Zusammenfassend lässt sich festhalten, dass durch eine Zertifizierung und die eigene Außendarstellung im Zusammenhang mit dem Gütesiegel keine falschen Erwartungen geweckt werden sollten, da der Vertrauensverlust der verschiedenen Interessensgruppen an einem Auskunftsportal nicht zu unterschätzen ist und eine existenzielle Gefahr darstellen kann.

6.3.6 Verantwortungsbereiche der teilnehmenden Unternehmen

Die Vertrauenswürdigkeit des Portals hängt entscheidend von zuverlässigen, korrekten Inhalten ab. Der Kernbereich der angebotenen Inhalte sind Musteranschreiben (vgl. 6.1.3.3). Ein Mehrwert für Betroffene kann darin bestehen, dass diese Auskunftsersuchen mit dem in einer Datei hinterlegten Namen des Adressaten und dessen Anschrift versehen werden können. Dies trägt wesentlich zur Attraktivität des Angebots des Portals bei. Zugleich übernimmt das Portal durch diesen Dienst eine erhebliche Verantwortung. Betroffene vertrauen auf die korrekte Adressierung. Sollten Fehler auftreten, entstehen für die Betroffenen Mehraufwende. Es muss etwa erneut Porto gelöst werden. Zudem kommt es zu zeitlichen Verzögerungen. Betroffene erwarten eine zügige Abwicklung des Auskunftsverfahrens. Insbesondere bedeutet eine Fehladressierung aber eine Fehlleitung möglicherweise sensibler, jedenfalls aber verifizierter Angaben der Betroffenen und führt zu einem erheblichen Vertrauensverlust. Um der übernommenen Verantwortung gerecht zu werden, muss das Portal erheblichen Rechercheaufwand betreiben. Die Bestände an Unternehmensadressen sind ständigen Qualitätskontrollen zu unterziehen.

Ein weiterer Ansatz besteht darin, primär die Unternehmen bzw. Organisationen selbst die Aktualität sicherstellen zu lassen. Wird eine entsprechende „Meldelösung“ eingesetzt, müssen mit den Unternehmen bzw. Organisationen vertragliche Vereinbarungen getroffen werden. Diese müssen insbesondere regeln, welche Angaben von ihnen zur Verfügung zu stellen sind und innerhalb welcher Frist Änderungen – vorzugsweise vorab – gemeldet bzw. selbst eingestellt werden müssen. Es sollte ein Kontaktweg zur Meldung von Fehlern wie veralteten oder fehlerhaften Adressen durch Dritte eingerichtet werden. Fehler würden von Nutzerinnen und Nutzern – evtl. auch trotz eines anderslautenden Hinweises – dem Portal zugerechnet werden. Daher sollten dem Portal sowohl Meldungen und Änderungsmeldungen der Unternehmen bzw. Organisationen als auch Fehlermeldungen zu Kontrollzwecken zugehen. Das Verfahren zur Bearbeitung von Fehlermeldungen muss verbindlich festgelegt sein. Insbesondere muss die Pflicht für das Unternehmen statuiert sein, Fehler unverzüglich zu beheben. Außerdem sind Konsequenzen für den Fall des Verstoßes gegen die Vereinbarungen festzulegen, die etwa in finanziellen Vertragsstrafen oder Veröffentlichungen bestehen können. Die Verantwortlichkeiten sind bei der Gestaltung des Portals abzubilden. Dies kann z. B. durch einen gut sichtbaren Hinweis auf die Verantwortlichkeit des Unternehmens bzw. der Organisation für die Aktualität der Adresse erfolgen.

7 Herausforderungen

Das Datenschutzrecht steht vor allem vor der Herausforderung, sich auf eine ständig schnellere Entwicklung der technischen Möglichkeiten der Datenverarbeitung einzustellen. An vielen Stellen wird der Vorwurf laut, die datenschutzrechtlichen Regularien würden den tatsächlichen Gegebenheiten nicht Herr. Dem kann vor dem Hintergrund des umfassenden datenschutzrechtlichen Regulierungssystems über das generelle Verbot mit Erlaubnisvorbehalt grundsätzlich nicht gefolgt werden. Für Bereiche allerdings, in denen das Datenschutzrecht Ansprüche vorsieht, wie etwa das Auskunftsrecht, muss genauer geprüft werden, ob diese für die Wahrung des grundgesetzlich verankerten Rechts auf informationelle Selbstbestimmung ausreichen. Denn Grundrechte verbürgen auch Gewährleistungsansprüche gegenüber dem Staat.

7.1 Auskunft über „blanke Daten“

Bereits im Volkszählungsurteil stellte das Bundesverfassungsgericht fest, dass es unter den Bedingungen automatisierter Datenverarbeitung kein belangloses Datum gibt.[79] Tatsächlich ist in der Datenverarbeitungspraxis festzustellen, dass die zunehmende Datenflut einen ansteigenden Bedarf an Datenselektion und -aggregation verursacht. „Blanke“ bzw. isolierte Daten verlieren an Bedeutung, vielmehr sind für die Wirtschaftspraxis Bewertungen anhand von Kontexten und Vergleichsgrößen von Relevanz. Eine bekannte Form der Aufbereitung ist das sog. Scoring, bei dem anhand von Erfahrungswerten hinsichtlich Vergleichsgruppen Wahrscheinlichkeitswerte für die Zukunft berechnet werden. Für diese spezielle Form der Datenverarbeitung wurden in § 34 Abs. 2, Abs. 4 BDSG im Rahmen der BDSG-Novelle I[80] des Jahres 2009 spezielle Auskunftsansprüche eingeführt. Es muss ausdrücklich u. a. über die Bedeutung der Wahrscheinlichkeitswerte und über die zur Berechnung genutzten Datenarten Auskunft erteilt werden. In den allgemeinen Auskunftsvorschriften insbesondere des § 34 Abs. 1 BDSG fehlen vergleichbar detaillierte Auskunftsvorgaben. Dies könnte den Schluss zulassen, dass im Übrigen, also außerhalb des Anwendungsbereichs der Abs. 2 und 4, keine entsprechend detaillierten Auskünfte zu erteilen sind. Dies erscheint allerdings bereits deshalb bedenklich, weil der Anwendungsbereich der allgemeinen Auskunftsvorschriften einen unbestimmbar weitreichenden Umfang umfasst.

Die Auskunftsansprüche des § 34 Abs. 2, Abs. 4 BDSG korrespondieren mit § 28b BDSG, wonach Scoring i. S. d. BDSG vorliegt, wenn zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Betroffenen ein Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten erhoben oder verwendet wird. Der Anwendungsbereich dieser Norm und der entsprechenden speziellen Auskunftsrechte könnte bereits in Frage stehen, wenn nicht ein Verhalten eines Betroffenen sondern beispielsweise seine Reputation bewertet werden soll. Ein Ausschluss der Sachverhalte, die nicht als Scoring i. S. d. BDSG einzuschätzen sind, von den detaillierten Auskunftsrechten des § 34 Abs. 2, Abs. 4 BDSG bzw. eine enge Aus-

[79] Urteil des Bundesverfassungsgerichts vom 15.12.1983 (Volkszählungsurteil), Az. 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, Rz. 152.

[80] Bundestag-Drucksachen 16/10529 und 16/10581 mit den Änderungen der Bundestag-Drucksache 16/13219.

legung der allgemeinen Auskunftsvorschriften ist allerdings nicht mit den schutzwürdigen Transparenzinteressen der Betroffenen vereinbar. Generell müssen Betroffene erfahren können, welche Bewertungen im weitesten Sinne zu den zur Person gespeicherten Daten vorgenommen werden. Ohnehin sind Werturteile ebenso wie Tatsachen vom Anwendungsbereich des BDSG erfasst.[81] Bewertungen können beispielsweise auf falschen Annahmen basieren. Sie bedürfen wie jede andere Form der Datenverwendung grundsätzlich der Kontrolle. Bei Bewertungen und anderen Formen der Datenaggregation kann u. a. aufgrund des Entstehungsprozesses und der generell bei automatisierter Datenverarbeitung erfahrungsgemäß bestehenden Plausibilitätsvermutung der Ergebnisse sogar von einem erhöhten Kontrollbedarf zur Wahrung der schutzwürdigen Interessen der Betroffenen ausgegangen werden. Denn es kann nicht ausgeschlossen werden, dass derartige Bewertungen, beispielsweise die Einordnung in eine Vergleichsgruppe (z. B. Frühbucher oder Kreditkarteninhaber) oder in eine sonstige Kategorie, wirtschaftliche Auswirkungen für den Betroffenen haben können wie etwa bei der Berechnung von Vertragskonditionen. Trotz alledem ist aus der aufsichtsbehördlichen Praxis bekannt, dass vielfach Auskünfte nach § 34 BDSG nur zu den „blanken Daten" bzw. „Rohdaten" erteilt werden. Die Rückschlüsse, die ein Unternehmen aus diesen Informationen über den Betroffenen zieht, ohne dieses Verfahren z. B. Scoring zu nennen, werden in der Regel nicht mitgeteilt. Ohnehin herrschen gewisse Unklarheiten hinsichtlich der Detailtiefe des Auskunftsanspruchs über die zu einer Person gespeicherten Daten nach § 34 Abs. 1 S. 1 Nr. 1 BDSG. Hier könnte eine gesetzliche Klarstellung Abhilfe schaffen.

Zudem darf nicht außer Acht gelassen werden, dass beispielsweise zu Zwecken der Werbung bestimmte personenbezogene Daten nach einem Gruppenmerkmal selektiert an Dritte weitergegeben werden können (§ 28 Abs. 3 S. 4 BDSG), sofern der Betroffene nicht widerspricht (§ 28 Abs. 4 BDSG). Aber auch wenn es zur Wahrung der berechtigten Interessen der verantwortlichen Stelle erforderlich ist und keine schutzwürdigen Interessen des Betroffenen entgegenstehen, kann beispielsweise grundsätzlich gem. § 28 Abs. 1 S. 1 Nr. 2 BDSG eine Übermittlung an Dritte zulässig sein. Die Verbreitung von Informationen birgt besondere Gefährdungen für die persönlichkeitsrechtlichen Interessen der Betroffenen.[82] Diese Gefährdung erhöht sich durch die Verbreitung von Bewertungen oder anderen Formen aggregierter Daten, da die Empfänger Informationen insbesondere aus automatisierter Datenverarbeitung erfahrungsgemäß für Tatsachen oder jedenfalls für belastbare Informationen halten. In diesem Kontext wären jedenfalls besondere Transparenzvorgaben erforderlich, wie detaillierte Benachrichtigungen des Betroffenen weitestgehend ohne Ausnahmeregelungen, die die derzeitige Gesetzeslage allerdings nicht bietet.

7.2 Selbstregulierung

Es stellt sich die Frage, ob die allgemeinen Herausforderungen des Datenschutzes und die unter 7.1 beispielhaft dargestellten Defizite im Bereich der Auskunftsrechte durch Selbstregulierung zu bewältigen sind. Derzeit wird Selbstregulierung jedenfalls an verschiedenen Stellen etwa von poli-

[81] Weichert in Däubler / Klebe / Wedde / Weichert (Hrsg.), Bundesdatenschutzgesetz Kompaktkommentar, 3. Auflage 2010, § 3 Rn. 17.

[82] BGH NJW 1966, S. 2353, 2354.

tischen Verantwortungsträgern als Lösung propagiert. So wurde beispielsweise im Jahr 2010 in den „14 Thesen zu den Grundlagen einer gemeinsamen Netzpolitik der Zukunft“[83] des Bundesinnenministeriums ausgeführt, es sollte soweit als möglich auf bestehende Regelungen zurückgegriffen und Selbstregulierungskräfte gestärkt werden. In diesem Zusammenhang ist zu konstatieren, dass erst im Jahr 2012 die Verhandlungen zur bisher einzigen Verhaltensregel einer Branche nach § 38a BDSG zu einem Ende kamen. Es stehen hierfür durchaus bereits gesetzliche Anknüpfungspunkte zur Verfügung. Doch obwohl für Branchenverbände die Möglichkeit besteht, die abstrakten datenschutzrechtlichen Regelungen mit Blick auf die konkreten Branchengegebenheiten zu konkretisieren und dies durch die Datenschutzaufsichtsbehörden auf die Vereinbarkeit mit dem Datenschutzrecht überprüfen zu lassen, wird diese Form der „regulierten Selbstregulierung“[84] nicht in der Breite angenommen. Dies könnte als Beleg dafür gelten, dass ohne zwingende Vorgaben insbesondere in gesetzlicher Form ein Engagement der Wirtschaft bei der Erstellung brachenspezifischer Regelungen nicht zu erwarten ist. Auch ein Engagement der Wirtschaft, die teilweise unklaren Auskunftsansprüche i. S. d. Rechts auf informationelle Selbstbestimmung des Einzelnen zu konkretisieren und sich selbst zu größtmöglicher Transparenz zu verpflichten, erscheint daher fernliegend. Zumal Selbstregulierung ohnehin bestimmte Defizite immanent sind.[85] Insbesondere ist das Instrument nicht geeignet, für die verantwortlichen Stellen einschränkende Standards durchzusetzen und umfassend fremde Interessen wie insbesondere die der Betroffenen einzubeziehen. Zudem können selbstgesetzte Regulierungen den Betroffenen nicht im selben Maße Vertrauen und Sicherheit bieten, da grundsätzlich keine Rechtsdurchsetzungsmöglichkeiten bestehen.

Eine teilweise lebendige und funktionierende Form der Datenschutzselbstregulierung besteht in der Zertifizierung datenschutzkonformer Produkte und Dienstleistungen. Zwar müssen unseriöse Anbieter vom Markt effektiv ferngehalten werden. Es existieren aber durchaus Erfolgsmodelle, deren Siegel für Unternehmen einen echten Wettbewerbsvorteil darstellen.

7.3 Weniger oder mehr Regulierungsbedarf?

Das aus den 1990er-Jahren stammende Datenschutzrecht kann die aktuellen und polarisierenden Fragen der Datenverwendung nicht adäquat beantworten.[86] Selbstregulierung kann für dieses Problem keine „automatische“, einfache Lösung liefern. Grundgesetzlich verankerte Werte wie

---

[83] Abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/thesen_netzpolitik.pdf;jsessionid=7B661F43F640935F840E1A39C68EF0E5.2_cid239?__blob=publicationFile (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

[84] Weichert in Däubler / Klebe / Wedde / Weichert (Hrsg.), Bundesdatenschutzgesetz Kompaktkommentar, 3. Auflage 2010, § 38a BDSG Rn. 1.

[85] Dr. Wolfgang Schulz „Selbstregulierung im Datenschutz – Erfahrungen und neue Ansätze“, Vortrag anlässlich der Konferenz am Safer Internet Day 2011, Folie 7. http://www.bmelv.de/SharedDocs/Downloads/Verbraucherschutz/Internet-Telekommunikation/Vortrag2011Schulz.pdf?__blob=publicationFile (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

[86] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, 33. Tätigkeitsbericht, 2011, Tz. 2. https://www.datenschutzzentrum.de/material/tb/tb33/kap02.htm (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

Freiheit und Selbstbestimmung kann dieser Ansatz nur gewährleisten, wenn ein verbindlicher gesetzlicher Rahmen die Grundlage bildet.

Die E-EU-DSGVO nimmt den Ansatz der regulierten Selbstregulierung auf. In Abschnitt 5 werden Verhaltensregeln und Zertifizierungen angesprochen. Art. 38 E-EU-DSGVO sieht insoweit vor, dass die Mitgliedstaaten, die Aufsichtsbehörden und die EU-Kommission die Ausarbeitung von Verhaltensregeln fördern werden, die nach Maßgabe der Besonderheiten der einzelnen Datenverarbeitungsbereiche zur ordnungsgemäßen Anwendung der E-EU-DSGVO beitragen sollen. In Hinblick auf Transparenzvorgaben und Auskunftsrechte ist von besonderem Interesse, dass als besondere Regelungsgegenstände u. a. faire und transparente Datenverarbeitung, Unterrichtung der Öffentlichkeit und der Betroffenen sowie Anfragen natürlicher Personen in Ausübung ihrer Rechte genannt werden. Eine zusätzliche Motivation, Branchenverhaltensregeln zu erstellen, könnte dadurch bewirkt werden, dass die Europäische Kommission die Ermächtigung erhalten soll, bestimmten Branchenverhaltensregeln Allgemeingültigkeit in der Europäischen Union zuzusprechen.

8 Innovative Ansätze und Forschungsfragen

Schon seit Jahren wird in der wissenschaftlichen Datenschutzdiskussion betont, dass ein Verbesserungsbedarf beim Wahrnehmen des Auskunftsrechts besteht und hierfür technische Unterstützung für die Betroffenen sinnvoll sein kann.[87] Dieser Abschnitt stellt einige Lösungsansätze vor und zeigt auf, wo weiterer Forschungsbedarf besteht.

8.1 Einzelnutzungsnachweise und (elektronischer) Datenbrief

Statt auf ein Aktivwerden des Betroffenen zu warten, könnten verantwortliche Stellen die Auskunft über die personenbezogenen Daten standardmäßig erteilen. Dies ist der Hintergrund für den vom Chaos Computer Club vorgeschlagenen „Datenbrief"[88], der anlassbezogen oder regelmäßig den Betroffenen zugestellt werden könnte. Das müsste nicht per Papierpost geschehen, sondern ginge auch elektronisch, sogar ohne Kenntnis der postalischen Adresse.

Eine ähnliche Idee wird von dem sog. „Einzelnutzungsnachweis"[89] verfolgt, der knapp zehn Jahre früher als der Datenbrief zur Diskussion gestellt wurde, aber kaum mediale Aufmerksamkeit erreichte. Der Einzelnutzungsnachweis zielt nicht nur auf eine Auskunft zu den personenbezogenen Daten ab, sondern soll die Datennutzungen durch die verantwortliche Stelle wie auf einem Kontoauszug oder einem Einzelverbindungsnachweis transparent machen. Bei diesem Ansatz wird deutlich, dass die Information in einem für den Betroffenen weiterverarbeitbaren und besser auswertbaren Format von Vorteil wäre. Eine Zustellung per verschlüsselter E-Mail oder per vom Betroffenen gesteuerten Abrufverfahren wäre durchaus denkbar.

Auf eine elektronische Fassung des Datenbriefs konzentriert sich ein weiterer Vorschlag, der ebenfalls eine Standardisierung eines Elektronischen-Datenbrief-Dienstes[90] anstrebt. Die rudimentären Ansätze einiger Telemedienanbieter, die eingeloggten Nutzerinnen und Nutzern in ihrem Kundenprofil Informationen über ihre Daten geben, reichen dazu nicht aus, weil sie nur Teile der vorhandenen Daten und der weiteren personenbezogenen Erkenntnisse über die Betroffenen sichtbar machen. Daher appelliert das Projekt „Elektronischer Datenbrief" an einer Weiterentwicklung in Form einer verbindlichen Richtlinie für die verantwortlichen Stellen.

---

87 ENISA Ad Hoc Working Group on Privacy & Technology, Technology-induced challenges in Privacy & Data Protection in Europe, Oktober 2008, S. 22 ff., http://www.enisa.europa.eu/activities/risk-management/files/deliverables/technology-induced-challenges-in-privacy-data-protection-in-europe (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

88 Chaos Computer Club, Datenbrief, 25.01.2010, http://www.ccc.de/datenbrief (Stand bzw. URL letztmals geprüft zum Veröffentlichungsdatum).

89 Köhntopp / Pfitzmann, Datenschutz Next Generation, in Bäumler (Hrsg.): E-Privacy – Datenschutz im Internet, 2000, S. 319 ff.

90 Heidisch / Pohlmann, Elektronischer Datenbrief – eine aktive informationelle Selbstbestimmung im Internet, Website Boosting, 03-04.2012, S. 94 u. 96.

8.2 Auskunftsersuchen unter Pseudonym

Wie bereits dargestellt (vgl. 2.3.3), besteht ein Auskunftsanspruch grundsätzlich bei der Verwendung von Pseudonymen. In diesem Fall können – je nach Art des Pseudonyms oder der Pseudonymisierung – allerdings Schwierigkeiten bei der Authentisierung bestehen: Handelt es sich bei dem Anfragenden wirklich um den Träger des Pseudonyms?

Problematisch sind in diesem Zusammenhang Pseudonyme, die nicht eindeutig einer natürlichen Person zugeordnet sind, beispielsweise Pseudonyme für eine Gruppe von Personen oder übertragbare Pseudonyme. Das Auskunftsrecht erstreckt sich lediglich auf die personenbezogenen Daten eines Individuums; eine Auskunftserteilung über fremde personenbezogene Daten hat zu unterbleiben. Diese Trennung ist jedoch bei der Verwendung von nicht-eindeutig zugeordneten Pseudonymen nicht möglich. In einigen Fällen erlauben Kontextinformationen die eindeutige Zuordnung: Beispielsweise werden dynamische IP-Adressen über die Zeit an viele Rechner vergeben; jedoch ist die Zuordnung zu einem definierten Zeitpunkt eindeutig. Für ein Auskunftsersuchen bei einem Anbieter von Telemedien wäre es denkbar, dass sich der Betroffene über einen Nachweis seiner IP-Adresse zu einem bestimmten Zeitpunkt authentisiert; eine Namensnennung wäre also nicht erforderlich. Allerdings würde die Behauptung des Betroffenen, er habe eine bestimmte IP-Adresse verwendet, nicht ausreichen, sondern der Nachweis müsste von einer Stelle erbracht werden, die dieses Wissen hat, z. B. der Internet Service Provider, und eine Manipulation müsste ausgeschlossen werden, z. B. durch eine elektronische Signatur. Zudem müsste die zeitliche Zuordnung authentisch sein, beispielsweise durch Einbindung eines Zeitstempeldienstes.

Einfacher zu handhaben sind Pseudonyme mit eindeutiger Zuordnung zu einer natürlichen Person und einer zuverlässigen Adressierungsmöglichkeit für die Antwort auf ein Auskunftsersuchen. Ein früher Prototyp einer pseudonymen E-Commerce-Nutzung mit Auskunftsfunktionalität wurde im Projekt „DASIT – Datenschutz in Telediensten“ entwickelt.[91]

Mit der Einführung des neuen Personalausweises ergibt sich die Möglichkeit für den Betroffenen, die eID-Funktion zur Authentisierung im Rahmen des Auskunftsersuchens zu nutzen. Im Fall einer Nutzung eines Angebots unter Pseudonym über das dienst- und kartenspezifische Kennzeichen des nPA könnte die Authentisierung für die Auskunft erfolgen, ohne dass außer dem Pseudonym weitere Nachweise erbracht werden müssten. Aus Datenschutzsicht ist dies ein wünschenswertes Feature, das grundsätzlich alle elektronischen Identitätsausweise mitbringen sollten.[92] Allerdings ist in der Realisierung des nPA das Pseudonym abhängig von dem Ausweis selbst, d. h. der Chipkarte. Bei einem Wechsel des nPA, beispielsweise im Falle eines Verlusts oder nach Ablauf der Gültigkeit, sind die verwendeten kartenspezifischen Pseudonyme nicht anschlussfähig.

---

[91] Enzmann / Scholz, Technisch-organisatorische Gestaltungsmöglichkeiten, in: Roßnagel (Hrsg.): Datenschutz beim Online-Einkauf – Herausforderungen, Konzepte, Lösungen, 2002, S. 77 ff.: Eine spezielle bei den Kundinnen und Kunden installierte Software, das sog. SET-Wallet (SET = Secure Electronic Transaction), ermöglichte den Online-Einkauf sowohl unter Angabe der Identitätsdaten als auch unter Pseudonym. Die Software sah eine Auskunftsfunktion vor, die sich ebenfalls auf die pseudonymen Daten erstreckte. Allerdings konnte sich der SET-Standard für Bezahlsysteme im Internet nicht durchsetzen. Das Projekt DASIT wurde von 1998 bis 2001 vom Bundesministerium für Wirtschaft und Technologie gefördert.

[92] Zwingelberg / Hansen, Privacy Protection Goals and Their Implications for eID Systems, in Camenisch et al. (Hrsg.): Privacy and Identity Management for Life, IFIP AICT 375, 2012, S. 255 f.

8.3 Betroffenenunterstützung über ein Identitätenmanagementsystem

Eine verallgemeinernde Variante der Nutzung eines Dienstes unter Pseudonym stellen nutzergesteuerte Identitätenmanagementsysteme dar. In allen Realisierungsvorschlägen spielt der Client auf Nutzerseite eine wesentliche Rolle. Beispielsweise wurde in den von der Europäischen Kommission geförderten Projekten „PRIME – Privacy and Identity Management for Europe" und „PrimeLife – Privacy and Identity Management in Europe for Life" ein als „Data Track" bezeichnetes Tool entwickelt und getestet, das die Transparenz für Nutzerinnen und Nutzer über die eigenen Online-Transaktionen erhöhen sollte, indem es die aus Datenschutzsicht wesentlichen Informationen clientseitig mitprotokollierte und auswertbar machte.[93] In einer erweiterten Fassung ermöglichte die prototypische „Data Track"-Software das Absenden elektronischer Auskunftsersuchen zu dem jeweils verwendeten Pseudonym. Auch eine halbautomatische Unterstützung des Auskunftsrechts der Nutzerinnen und Nutzer durch Darstellen der Adresse der verantwortlichen Stelle oder der zuständigen Aufsichtsbehörde im Falle einer fehlenden oder unbefriedigenden Antwort war vorgesehen.[94]

Allerdings birgt eine clientseitige Realisierung vielfältige Herausforderungen, gerade wenn – wie im Falle des „Data Tracks" – eine erhebliche Menge an aussagekräftigen personenbezogenen Daten verarbeitet werden: Wie können diese Daten angesichts der heutzutage inhärent unsicheren Endgeräte wie PCs, Tablets oder Smartphones gegen unberechtigtes Auslesen, Manipulieren oder Löschen wirksam geschützt werden? Wie stellt man sicher, dass notwendige Updates der Client-Software erfolgen, aber durch die Update-Möglichkeit keine zusätzlichen Risiken für Datenschutz und Datensicherheit entstehen? Wer übernimmt die Verantwortung für ein reibungsloses Zusammenspiel zwischen Hardware, Betriebssystem, Anwendungssoftware und zusätzlich installierten Datenschutz-Tools, die bei jeder Kommunikation und bei jedem Datenzugriff eingebunden sein müssen? Wie kann man den Aufwand für die Pflege solcher Tools, die möglichst für alle Plattformen zur Verfügung stehen sollten, gering halten? Wie realisiert man ein ausreichend hohes Maß an Usability für Datenschutz- und Transparenzfunktionalität gerade in Hinblick auf die Vielzahl von eingebundenen Dienstleistern in heutiger Internet-Kommunikation? Und wie können die Entwicklung und der Betrieb solcher Datenschutz-Services mit dem erwarteten Level an Professionalität finanziert werden?

Es wird deutlich, dass hier noch erheblicher Forschungs- und Entwicklungsbedarf besteht. Eine „Quick&Dirty"-Lösung, beispielsweise per App für ein Smartphone, könnte zumindest die Erwartungen an nutzergesteuerte Identitätenmanagementsysteme bei weitem nicht erfüllen. Teillösungen, z. B. rein für das Stellen von Auskunftsersuchen, wären weniger aufwendig und auch leichter abzusichern, doch auch hier bestünde ein Pflegeaufwand für verschiedene Plattformen sowie im Fehlerfall bei vielen Nutzerinnen und Nutzern die Erwartung an den Betrieb eines Helpdesks, woraus weitere Kosten resultieren.

---

[93] Fischer-Hübner et al., Human-Computer Interaction, in Camenisch et al. (Hrsg.): Digital Privacy, LNCS 6545, 2011, S. 587 ff.

[94] Hansen, Marrying Transparency Tools With User-Controlled Identity Management, in Fischer-Hübner et al. (Hrsg.): The Future of Identity in the Information Society, IFIP Vol. 262, 2008, S. 211 ff.

8.4 Ubiquitäre Datenverarbeitung und Wahrnehmung des Auskunftsrechts

Eine gänzlich verschiedene Herausforderung ergibt sich in der Welt des Ubiquitous Computing (allgegenwärtige Datenverarbeitung) mit Sensoren und Aktuatoren in Cyber-Physical Systems, die sich in allen Lebensbereichen einbauen lassen. Die Durchdringung der Umgebung mit Sensorik, wie dies in sog. „intelligenten Häusern" schon ausprobiert wird und beim „Ambient Assisted Living" u. a. im medizischen und pflegerischen Kontext immer mehr Verbreitung finden wird, erfordert andere Herangehensweisen für die Information der Betroffenen.[95]

Vielfach werden Cyber-Physical Systems als Ganzes oder Teilsysteme bestehend aus Sensoren oder Aktuatoren personenbezogene Daten nicht dauerhaft speichern müssen, sondern werten sie sofort aus und lösen entsprechende Datenverarbeitungs- oder Steuerungsprozesse aus. Hier ist eine sofortige oder Vorabinformation der Betroffenen erforderlich. Auch die Benutzungsschnittstellen werden sich ändern müssen: Smartphones oder Datenbrillen könnten durch visuelle oder akustische Signale die Betroffenen auf eine geplante oder laufende Datenverarbeitung hinweisen; auch die Umgebung selbst könnte auf geeignete Weise informieren.

Die Forschung in diesem Bereich – auch zu Datenschutz und Datensicherheit – betrifft einen sehr viel größeren Bereich als nur die Wahrnehmung des Auskunftsrechts. Neben den Transparenzanforderungen werden insbesondere Interventionsmöglichkeiten für den Betroffenen wichtig sein, um das Recht auf informationelle Selbstbestimmung wahrnehmen zu können.[96] Dies sollte bereits in der frühen Phase der Entwicklung und Standardisierung Beachtung finden.

[95] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD) / Humboldt-Universität zu Berlin, TAUCIS – Technikfolgenabschätzung: Ubiquitäres Computing und Informationelle Selbstbestimmung, Studie im Auftrag des Bundesministeriums für Bildung und Forschung, 2006, S. 214, 224 f., 227 f. u. 235.

[96] Geisberger / Broy (Hrsg.), agendaCPS – Integrierte Forschungsagenda Cyber-Physical Systems, acatech Studie, Springer, März 2012, S. 122 ff.

9 Fazit

Die Realisierung eines vertrauenswürdigen, nachhaltigen Auskunftsportals ist ein anspruchsvolles Vorhaben. Grund dafür sind die spezifischen Erwartungen, die an ein solches Portal gestellt werden. Durch den „Geschäftszweck", den sich das Auskunftsportal gibt, ist es in besonderer Weise zur Beachtung der Grundsätze des Datenschutzes, aber auch zu einem überobligatorischen Schutz der Betroffenen verpflichtet. Oberste Prämissen bei der Ausgestaltung des Portals sowie bei der Auswahl und Gestaltung der Datenverarbeitungssysteme müssen Förderung von Transparenz und Datensparsamkeit sein. Risiken für die Nutzerinnen und Nutzer müssen effektiv ausgeschlossen werden. Ein diese Grundsätze konsequent beachtendes Konzept ist eine der wesentlichen Voraussetzung für den Erfolgs eines solchen Portals. Durch die Unterstützung und den Einsatz innovativer datenschutzfreundlicher Techniken kann bei der relevanten Zielgruppe Aufmerksamkeit erlangt werden.

Ein positiver gesellschaftlicher Effekt eines Auskunftsportals besteht darin, dass es die Bekanntheit des bestehenden Auskunftsrechts in der Öffentlichkeit erhöht. Außerdem kann es die Betroffenen bei der Wahrnehmung des Auskunftsrechts in vielfältiger Weise unterstützen. Die Mittel hierzu sollten stets einem ganzheitlichen Datenschutzansatz folgen.

Die bestehenden gesetzlichen Auskunftsansprüche lassen Raum für Verbesserungen. Insbesondere der Anspruch auf Auskunft hinsichtlich der „blanken" gespeicherten Daten scheint in einer digitalen Welt nicht mehr dem Schutzbedarf des Einzelnen zu entsprechen. Auch jenseits von Scorewerten finden Bewertungen und Kategorisierungen statt. Eine Kenntnis über diese Einordnung ist Bedingung für eine tatsächliche Transparenz und damit auch für die informationelle Selbstbestimmung. Solche und ähnliche Schwachpunkte könnte ein vertrauenswürdiges, akzeptiertes Auskunftsportal an zentraler Stelle dokumentieren und aus erster Hand in die aktuelle gesellschaftliche Diskussion etwa zu einem neuen Datenschutzrecht einbringen.

Abkürzungsverzeichnis

§	Paragraf
§§	Paragrafen
a. A.	andere Ansichten
Abs.	Absatz
AG	Aktiengesellschaft
AG	Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
AktG	Aktiengesetz
AO	Abgabenordnung
Az.	Aktenzeichen
BBG	Bundesbeamtengesetz
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BfDI	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BLE	Bundesanstalt für Landwirtschaft und Ernährung
BMELV	Bundesministeriums für Ernährung, Landwirtschaft und Verbraucherschutz
BVerfG	Bundesverfassungsgericht
bzw.	beziehungsweise
DASIT	Datenschutz in Telediensten (Projekt von 1998 bis 2001)
d. h.	das heißt
DoS	Denial of Service
E-EU-DSGVO	Entwurf einer Europäischer Datenschutz-Grundverordnung
EG	Europäische Gemeinschaft
EG-DSRL	Europäische Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995
eID	elektronischer Identitätsnachweis
EuGH	Gerichtshof der Europäischen Union
f., ff.	folgende
FAQ	Frequently Asked Questions

gem.	gemäß
GG	Grundgesetz
ggf.	gegebenenfalls
GmbH	Gesellschaft mit beschränkter Haftung
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
Hrsg.	Herausgeber
HGB	Handelsgesetzbuch
IP	Internet Protocol
Ipv4	Internet Protocol Version 4
i. S. d.	im Sinne der / des
i. S. e.	im Sinne eines
i. V. m.	in Verbindung mit
KWG	Kreditwesengesetz
LDSG	Landesdatenschutzgesetz
LG	Landgericht
m. w. N.	mit weiteren Nachweisen
nPA	elektronischer Personalausweis / neuer Personalausweis
NPO	Non-Profit-Organisation
Nr.	Nummer
o. Ä.	Oder Ähnliches
OLG	Oberlandesgericht
PauswG	Personalausweisgesetz
PET	Privacy–Enhancing Technologies
PRIME	Privacy and Identity Management for Europe (Projekt von 2004 bis 2008)
PrimeLife	Privacy and Identity Management in Europe for Life (Projekt von 2008 bis 2011)
QR	Quick Response
Rn.	Randnummer
Rz.	Randziffer
S.	Satz
S.	Seite
SET	Secure Electronic Transaction

SGB	Sozialgesetzbuch
sog.	so genannt
SSL	Secure Sockets Layer
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
Tz.	Textziffer
u.	und
u. a.	unter anderem
VfB	Vergabestelle für Berechtigungszertifikate
vgl.	vergleiche
ZPO	Zivilprozessordnung
z. B.	zum Beispiel

Literaturverzeichnis

Chaos Computer Club (frankro)	Datenbrief, 25.01.2010, http://www.ccc.de/datenbrief
Däubler, Wolfgang / Klebe, Thomas / Wedde, Peter / Weichert, Thilo (Hrsg.)	Bundesdatenschutzgesetz Kompaktkommentar, Frankfurt am Main, 3. Auflage 2010.
ENISA Ad Hoc Working Group on Privacy & Technology	Technology-induced challenges in Privacy & Data Protection in Europe, Oktober 2008.
Enzmann, Matthias / Scholz, Philip	Technisch-organisatorische Gestaltungsmöglichkeiten, in: Roßnagel, Alexander (Hrsg.): Datenschutz beim Online-Einkauf – Herausforderungen, Konzepte, Lösungen, Vieweg, 2002, S. 73-88.
Fischer-Hübner, Simone / Pettersson, John Sören / Bergmann, Mike / Hansen, Marit / Pearson, Siani / Casassa Mont, Marco	Human-Computer Interaction, in: Jan Camenisch, Ronald Leenes, Dieter Sommer (Hrsg.): Digital Privacy, LNCS 6545, Springer, 2011, S. 569-595.
Geisberger, Eva / Broy, Manfred (Hrsg.)	agendaCPS – Integrierte Forschungsagenda Cyber-Physical Systems, acatech Studie, Springer, März 2012.
Gola, Peter / Schomerus, Rudolf	BDSG Bundesdatenschutzgesetz Kommentar, München, 9. Auflage, 2012.
Grimm, Rüdiger / Löhndorf, Nils / Roßnagel, Alexander	E-Commerce meets E-Privacy, in: Helmut Bäumler (Hrsg.): E-Privacy – Datenschutz im Internet, 2000, S. 133-140.
Hansen, Marit	Marrying Transparency Tools With User-Controlled Identity Management, in: Simone Fischer-Hübner et al. (Hrsg.): The Future of Identity in the Information Society, IFIP Vol. 262, Springer, 2008, S. 199-220,
Heidisch, Maik / Pohlmann, Norbert	Elektronischer Datenbrief – eine aktive informationelle Selbstbestimmung im Internet, Website Boosting, Nürnberg, 03-04.2012, S. 92-96.
Hoeren, Thomas / Sieber, Ulrich (Hrsg.)	Handbuch Multimedia-Recht. Rechtsfragen des elektronischen Geschäftsverkehrs.

Imberg, Alexander P. / Geissl, Karin E.	Dokumentenmanagementrichtlinien und Aufbewahrungspflichten im Hinblick auf die rechtlichen Anforderungen des U.S. Zivilverfahrens, in: Corporate Compliance Zeitschrift (CCZ) 2009, S. 190-193.
Köhntopp, Marit / Pfitzmann, Andreas	Datenschutz Next Generation, in: Helmut Bäumler (Hrsg.): E-Privacy – Datenschutz im Internet, 2000, S. 316-322.
Meints, Martin	Datenschutz durch Prozesse, in: DuD 2007, S. 91-95.
Palandt, Otto	Bürgerliches Gesetzbuch, München, 69. Auflage 2010.
Simitis, Spiros (Hrsg.)	Kommentar zum Bundesdatenschutzgesetz (BDSG), Baden-Baden, 7. Auflage 2011.
Taeger, Jürgen / Gabel, Detlev (Hrsg.)	Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, Frankfurt am Main, 1. Auflage, 2010.
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)	Erhöhung des Datenschutzniveaus zugunsten der Verbraucher, Studie im Auftrag des Bundesministeriums für Verbraucherschutz, Ernährung und Landwirtschaft, 2006.
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)	33. Tätigkeitsbericht, 22.03.2011.
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD) / Humboldt-Universität zu Berlin	TAUCIS – Technikfolgenabschätzung: Ubiquitäres Computing und Informationelle Selbstbestimmung, Studie im Auftrag des Bundesministeriums für Bildung und Forschung, 2006.
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD) / Technische Universität Dresden	Verkettung digitaler Identitäten, Report im Auftrag des Bundesministeriums für Bildung und Forschung, Kiel, 2007.
Zwingelberg, Harald / Hansen, Marit	Privacy Protection Goals and Their Implications for eID Systems, in: Jan Camenisch et al. (Hrsg.): Privacy and Identity Management for Life, IFIP AICT 375, S. 245-260, 2012.

Dokumente

AG Hamburg-Altona	Urteil Az. 317 C 338/04, 17.11.2004.
Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder	Orientierungshilfe „Protokollierung“, Stand 02.11.2009.
Artikel-29-Datenschutzgruppe	Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen, WP 148, S. 23.
Bundesamt für Sicherheit in der Informationstechnik (BSI)	IT-Grundschutz-Kataloge, Bonn.
Bundesgerichtshof	Urteil Az. I ZR 39/89, 04.10.1990.
Bundesgerichtshof	BGH NJW 22.05.1984, S. 1886 ff.
Bundesgerichtshof	BGH NJW 16.09.1966, S. 2353 ff.
Bundesministerium des Innern	14 Thesen zu den Grundlagen einer gemeinsamen Netzpolitik der Zukunft, 22.06.2010
Bundesrat	Bundesrats-Drucksache 550/08, 08.08.2008.
Bundestag	Bundestag-Drucksache 16/10529, 10.10.2008.
Bundestag	Bundestag-Drucksache 16/10581, 15.10.2008.
Bundestag	Bundestag-Drucksache 16/13657, 01.07.2009.
Bundestag	Bundestag-Drucksache 16/13219, 27.05.2009.
Bundesverfassungsgericht	Urteil vom 24.11.2010, Az. 1 BvF 2/05.
Bundesverfassungsgericht	Volkszählungsurteil, Urteil vom 15.12.1983, Az. 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83.
Deutsches Institut für Normung e.V. (DIN)	Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten.

Düsseldorfer Kreis	Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten, 27.11.2009.
Düsseldorfer Kreis	Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, Bonitätsauskünfte über Mietinteressenten nur eingeschränkt zulässig, 22.10.2009.
Entwurf Europäische Datenschutz-Grundverordnung	Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), 25.01.2012.
Europäischer Gerichtshof	Urteil Az. C-553/07 (Rijkeboer), 07.05.2009.
Landgericht Berlin	Urteil Az. 6 O 479/10, 01.11.2011.
Landgericht Darmstadt	Urteil Az. 22 O 100/08, 24.11.2008.
Landgericht Köln	Urteil Az. 31 O 491/11, 05.01.2012.
Landgericht Ulm	Urteil Az. 1 S 89/04, 01.12.2004 in DuD 2005, S. 100-103.
Oberlandesgericht Dresden	Urteil Az. 14 U 167/12, 03.07.2012.
Oberlandesgericht Frankfurt	Beschluss Az. 6 W 16/94, 08.03.1994.
Richtlinie 2002/58/EG geändert durch Richtlinie 2009/136/EG	Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation, E-Privacy-Richtlinie), ABl. EG Nr. L 201 vom 31.07.2002, S. 37-47 geändert durch Richtlinie 2009/136/EG, ABI. EG Nr. L 337 vom 25.11.2009, S. 11-36.

Richtlinie 95/46/EG — Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABL. EG Nr. L 281 vom 23.11.1995, S. 31-50, (EG-Datenschutzrichtlinie).

Schufa Holding AG — Pressemitteilung zum Anstieg der Selbstauskünfte bei der Schufa nach der Änderung des BDSG, 19.05.2010.

Schulz, Wolfgang — „Selbstregulierung im Datenschutz – Erfahrungen und neue Ansätze“, Vortrag anlässlich der Konferenz am Safer Internet Day 2011.