IHR GUTES RECHT IM DATENSCHUTZ

WIE SIE SICH GEGEN ANGRIFFE AUF IHRE PRIVATSPHÄRE WEHREN

INHALT

DATENSCHUTZ IST EINE DER GRÖSSTEN HERAUSFORDERUNGEN UNSERER ZEIT

2013 nutzen 19 Millionen Deutsche täglich Facebook, Google+ wuchs im Zeitraum eines Jahres in Deutschland kontinuierlich um über 80 Prozent auf 6,7 Millionen aktive Nutzer. In einem Jahr sind die Besucherzahlen von Pinterest in Deutschland um 181 Prozent auf 864.000 gestiegen. Bei der Nutzung von Social-Media-Kanälen und weiteren Aktivitäten im Netz fallen riesige Datenmengen an, die weltweit gebündelt, ausgelesen und sowohl von Unternehmen wie auch Privatpersonen nach bestimmten Kriterien analysiert werden können.

Mit der Preisgabe privater, sogar intimer Informationen in sozialen Medien stellt sich die Frage, ob den Menschen ihre Privatsphäre noch wichtig ist? Und wenn ja, ist der Schutz der Privatsphäre überhaupt noch möglich und wünschenswert? Wissen die Nutzer überhaupt um den Wert ihrer Daten für die Unternehmen, die vermeintlich kostenlose Dienste zur Verfügung stellen?

Diese Broschüre will Sie aufklären – über Ihre Rechte in der digitalen Welt und wie Sie diese wahrnehmen können. Und Sie werden überrascht sein, wie viele Möglichkeiten Sie eigentlich haben.

SIE HABEN MEHR RECHTE, ALS SIE DENKEN

Der Datenschutz hat durch das berühmte Volkszählungsurteil von 1983 die verfassungsrechtlichen Weihen eines Grundrechts erhalten („Recht auf informationelle Selbstbestimmung“). Für alltägliche Probleme und Fragen des Datenschutzes und seiner Durchsetzung ist das Verfassungsgericht aber zu weit weg. Wie auch in allen anderen Bereichen des Lebens ist es zunächst Aufgabe eines jeden Einzelnen, sich um die Wahrung und Verteidigung seiner Rechte selbst zu kümmern. Mittel hierzu sind ein datenschutzbewusstes Verhalten und Selbstdatenschutz, aber auch das Gewusst-wie, wenn man sich in seinen Datenschutzrechten verletzt fühlt und sich wehren will. Denn auch Datenschutzansprüche können auf juristischem Wege durchgesetzt werden. Problematisch ist aber, dass die meisten Datenschutzverstöße für den Einzelnen in der Regel weit davon entfernt sind, so störend oder eingreifend zu sein, dass es sich wirtschaftlich oder emotional lohnen würde, dagegen vorzugehen.

Man nennt dieses Phänomen „rationale Apathie“. Ebenfalls problematisch für die individuelle Durchsetzung des Datenschutzes ist der Umstand, dass ein Eingriff nicht fühlbar ist und deshalb nur schwer und oft erst verzögert bemerkt wird.

Diesen beiden Besonderheiten im Datenschutz versucht das Datenschutzrecht entgegenzuwirken, vor allem durch umfangreiche Informationspflichten der verantwortlichen Stelle gegenüber dem Betroffenen und durch institutionelle Hilfestellung bei der Durchsetzung datenschutzrechtlicher Ansprüche.

Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Absatz 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. (1. Leitsatz der Volkszählungsentscheidung des Bundesverfassungsgerichts vom 15. Dezember 1983, Amtliche Sammlung Bd. 65, S. 1).

RECHT BEKOMMT NUR DER, DER ES FORDERT

Wie in der realen Welt, so müssen Sie auch in der digitalen nicht alles hinnehmen. Werden Ihr Bild, Ihre Adresse oder sonstige Daten von Ihnen ohne Ihre Zustimmung oder, ohne dass ein Gesetz besteht, verwendet, in einen falschen Zusammenhang gebracht oder in unrechtmäßiger Weise gebraucht, können Sie dagegen vorgehen. Als Erstes sollten Sie immer die Umstände und den Umfang eines Datenschutzeingriffs feststellen. Um rechtlich vorzugehen, müssen Sie die verantwortliche Stelle identifizieren. Denn ohne eine „ladungsfähige Anschrift" laufen die Mühlen der Justiz nicht an.

TRANSPARENZ IST PFLICHT

[1] § 5 TMG; § 55 RStV.
[2] § 4 g Absatz 2 Satz 2 BDSG.
[3] § 42 a BDSG; § 109 a TKG; § 15 a TMG.

Der erste Schritt zur Datenschutzdurchsetzung ist dadurch erleichtert, dass die allgemeinen Informationspflichten der Betreiber von Websites und digitalen Angeboten recht umfassend sind. Jede Website muss mit einem Impressum versehen sein, das von der Startseite direkt zugänglich ist.[1] Findet sich kein Impressum, so ist das Webangebot schon rechtlich unsauber und kann beanstandet werden. Im Impressum finden Sie die Verantwortlichen und die Anschrift des Webangebotes. Auch in der Offline-Welt reichen die Informationen von Datenschutzerklärungen und Privacy Policies bis zu den Verarbeitungsverzeichnissen[2], mittels derer Sie den Geschäftsgegenstand bzw. die Verwaltungstätigkeit eines Unternehmens oder einer Behörde grob einschätzen können. Zusätzlich sind Datenverarbeiter seit einiger Zeit gezwungen, die Öffentlichkeit über Datenpannen zu unterrichten.[3] Alle, die mit Daten umgehen, sind also in der Bringschuld, weitgehende Transparenz über den Umgang und Zweck ihrer Datensammlung herzustellen.

Auf der Grundlage dieser Informierungspflicht bei Datenlecks mussten in der letzten Zeit Spielkonsolenbetreiber und Mobilfunkunternehmen, die Opfer erfolgreicher Hacking-Attacken geworden waren, dies ihren Kunden und der Öffentlichkeit mitteilen.

WER DATEN ERHEBT, MUSS DARÜBER INFORMIEREN

Was vielen nicht bewusst ist: Wer Daten von Ihnen verwendet, muss Sie entweder vorher darüber unterrichten oder davon in Kenntnis setzen, wenn Sie nicht ohnehin schon Bescheid wissen. Im Normalfall muss Sie die „verantwortliche Stelle" bei der Datenerhebung über die wesentlichen Umstände informieren.[1] Wenn die Daten nicht bei Ihnen selbst erhoben werden, sondern über Dritte, tritt an die Stelle der Unterrichtung die nachträgliche Benachrichtigung.[2] Leider kennt die Benachrichtigungspflicht aber eine lange Reihe von Ausnahmen, die auf Bagatellsachverhalte und auf Geheimnisschutz Rücksicht nehmen.

[1] § 4 Absatz 3 BDSG.
[2] § 19 a, § 33 BDSG.

VERLANGEN SIE AUSKUNFT

Daher gibt es Unternehmen und Behörden, die ihrer Informationspflicht nicht nachkommen oder sich auf eine gesetzliche Ausnahme berufen können. Wenn Sie weder unterrichtet noch benachrichtigt wurden, können Sie von Ihrem Auskunftsrecht[1] Gebrauch machen.

Ob die Ausnahmen zu weit gefasst sind, wird aktuell rechtspolitisch diskutiert.

[1] § 19, § 34 BDSG.

GEHEN SIE DEM RECHT AUF DEN GRUND

Oft hat man das Gefühl, ungerecht behandelt zu werden. Aber ein Unrechtsgefühl ist noch kein juristischer Tatbestand. Erst wenn tatsächlich ein Rechtsverstoß vorliegt, können Sie auch dagegen vorgehen. Den Abgleich von Unrechtsgefühl mit der Rechtslage nennen die Juristen „Subsumtion". Sie müssen aber keine zwölf Semester Jura studiert haben, um Gesetzesverstöße erkennen zu können. Um sich in den Gesetzen zurechtzufinden, muss man:

- deren Anwendungsbereich,
- deren innere Struktur
- und die Grundbegriffe des Datenschutzrechts kennen.

Dies wird im folgenden Abschnitt beschrieben.

DATENSCHUTZ FÜR EINSTEIGER

Was ist Datenschutz eigentlich genau? Allgemein und umgangssprachlich wird manchmal auch der Schutz vor Industriespionage oder sogar das Wegschließen des Tagebuches vor den Eltern als „Datenschutz" bezeichnet. In der bürokratisch-spröden Terminologie des Datenschutzrechts bezieht sich das Gesetz aber nur auf „personenbezogene Daten" eines „Betroffenen" bei einer „verantwortlichen Stelle" mit einem Bezug zu Deutschland.

Wer ist „Betroffener"?

„Betroffene"[1] sind alle natürlichen Personen, also neben Verbrauchern auch Freiberufler und Einzelunternehmer. Staatsangehörigkeit und Alter sind nicht relevant.

[1] § 3 Absatz 1 BDSG.

Was sind „personenbezogene Daten"?

Als „personenbezogene Daten"[1] werden alle Angaben erfasst, die sich auf Sie beziehen oder mit einem gewissen Aufwand auf Sie bezogen werden können. Zweifelsfälle ergeben sich dann, wenn Daten mehreren Personen zugleich zugeordnet werden können, wie zum Beispiel bei Angaben über Ehegatten und bei statistischen Wahrscheinlichkeitsaussagen.

„Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)." (§ 3 Absatz 1 BDSG)

[1] Ebenfalls § 3 Absatz 1 BDSG.

Wer ist eine „verantwortliche Stelle"?

Das Datenschutzrecht beschränkt sich auf die Datenverarbeitung durch „verantwortliche Stellen"[1]. Darunter fallen nur behördliche und kommerzielle Datenverarbeiter. Private Datenverarbeitung, wie zum Beispiel durch eigene Kalender, Listen und Korrespondenz, werden normalerweise nicht vom Datenschutzrecht berührt. Betreiben Privatpersonen allerdings Websites, auf denen sie Daten von anderen verwenden, müssen sie sich ebenfalls an das Datenschutzrecht halten.

„Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt." (§ 3 Absatz 7 BDSG)

[1] § 3 Absatz 7 BDSG.

Wann gilt deutsches Recht?

Das deutsche Datenschutzrecht ist nicht weltweit anwendbar. Die verschiedenen Länder haben zum Thema Datenschutz unterschiedliche Auffassungen. So sind die Datenschutzgesetze in den USA zum Beispiel vergleichsweise locker. Ganz einfach ist der Fall, wenn die Daten eines Deutschen in Deutschland von einer deutschen verantwortlichen Stelle erhoben werden. Komplizierter wird es, wenn die verantwortliche Stelle im Ausland sitzt. Hier ist ausschlaggebend für das Bundesdatenschutzgesetz, ob die „Datenverarbeitungsanlage" sich in Deutschland befindet. Das ist zum Beispiel der Fall, wenn das Unternehmen, das Ihre Daten verarbeitet, ein Rechenzentrum in Deutschland hat. Leider lässt sich dies in den meisten Fällen mit einem Blick ins Impressum nicht klären. Liegt der Geschäftssitz in der Europäischen Union (EU), dann gilt das Recht des jeweiligen Landes. Hier ist das Impressum dann als Informationsquelle wieder hilfreich.

„Dieses Gesetz findet keine Anwendung, sofern eine in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegene verantwortliche Stelle personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, es sei denn, dies erfolgt durch eine Niederlassung im Inland. Dieses Gesetz findet Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt." (§ 1 Absatz 5 Sätze 1 und 2 BDSG)

[1] § 1 Absatz 5 BDSG.

Das Bundesdatenschutzgesetz ist in gewisser Weise ein Grund-Gesetz des deutschen Datenschutzes, neben dem Bund, Länder und die EU weitere Regelungen erlassen haben.

Vereinfacht kann man sagen, dass die Länder für ihre Verwaltungsbehörden zuständig sind und der Bund für die Bundesbehörden sowie für den Bereich der Wirtschaft einschließlich der Arbeitsverhältnisse. In Europa wurde zwar 1995 die allgemeine EG-Datenschutzrichtlinie erlassen. Die macht sich aber nur in Gestalt der mitgliedstaatlichen Einzelgesetzgebung bemerkbar, für uns also durch die deutschen Datenschutzgesetze. Die seit 2012 diskutierte EU-Datenschutz-Grundverordnung wird dies alles grundlegend ändern, soweit sie das bisherige europäische und das mitgliedstaatliche Recht ersetzt.

Datenschutzrecht ist nicht gleich Datenschutzrecht

Das BDSG sowie eine kommende EU-Datenschutz-Grundverordnung regeln aber nicht das gesamte Datenschutzrecht. Vielmehr wird das allgemeine Datenschutzrecht durch viele „bereichsspezifische Regelungen" ergänzt. Das Gleiche gilt übrigens auch für die Datenschutzgesetze der Länder. So ist der Datenschutz bei den Sicherheitsbehörden in der Strafprozessordnung (StPO) und in den Polizei- und Nachrichtendienstgesetzen geregelt. Der Internetdatenschutz ist (hauptsächlich) im Telekommunikationsgesetz (TKG), im Telemediengesetz (TMG) sowie in europäischen Verordnungen verankert. Das bereichsspezifische Werbedatenschutzrecht ist dagegen Teil des BDSG.[1] Auch der Beschäftigtendatenschutz ist dort, wenngleich nur im Ansatz, in § 32 BDSG geregelt. Er beruht darüber hinaus aber vorwiegend auf Richterrecht.

[1] § 28 Absatz 3 BDSG.

Das Datenschutzrecht, das im BDSG normiert ist, spaltet sich noch einmal in zwei Teilbereiche auf. Durch das BDSG hindurch zieht sich die Unterscheidung zwischen dem „öffentlichen Bereich"[1] und dem sogenannten „nichtöffentlichen Bereich"[2]. Grenzfälle sind Stadtwerke und Sparkassen. Insoweit beinhaltet das BDSG „zwei Gesetze in einem", die allerdings viele Gemeinsamkeiten haben.

[1] (Bundes-)Verwaltung; §§ 12 ff. BDSG.
[2] Privatwirtschaft; §§ 27 ff. BDSG.

Traum von einer einheitlichen Gesetzgebung

Leider ist das deutsche Datenschutzrecht nicht wirklich übersichtlich. Es ist horizontal und vertikal gegliedert, zudem auch thematisch verteilt. In einigen Fällen wird es nicht leicht sein, das für den jeweiligen Fall anwendbare Recht zu finden. Insgesamt hat man es oft mit Fällen zu tun, in denen Normen aus mehreren Gesetzen zusammengetragen werden müssen: So bestimmt sich zum Beispiel die Rechtmäßigkeit von Direktmarketing aus der Zusammenschau der Datenschutzregeln des BDSG[1] und des Belästigungsschutzes nach Wettbewerbsrecht.[2] Im Beschäftigtendatenschutz gelten § 32 BDSG, Richterrecht und die individuell ausgehandelten Betriebsvereinbarungen zwischen Arbeitgeber und Betriebsrat. Die Datenverarbeitung der Polizei (Personenkontrollen, Videoüberwachung, Lauschangriff) richtet sich für die Fahndung nach Straftätern nach der Strafprozessordnung (StPO) des Bundes. Bei der Gefahrenabwehr (Polizei als „Freund und Helfer") greifen jedoch die Polizeigesetze der Länder. Die deutschen Nachrichtendienste arbeiten nach jeweils spezifischen Vorschriften (Gesetz über den Bundesnachrichtendienst, BNDG; Bundesverfassungsschutzgesetz, BVerfSchG; Gesetz über den Militärischen Abschirmdienst, MADG).

[1] § 28 Absatz 3 BDSG.
[2] § 7 UWG.

DIE VERWENDUNG IHRER DATEN IST EIGENTLICH VERBOTEN

„Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.“ (§ 4 Absatz 1 BDSG)

[1] § 4 Absatz 1 BDSG.

Was die wenigsten wissen: Das Bundesdatenschutzgesetz verbietet die Verwendung Ihrer persönlichen Daten – bis Sie oder das Gesetz es ausdrücklich erlauben. Das „Verbot mit Erlaubnisvorbehalt“[1] bedeutet, dass eine Verarbeitung von Ihren personenbezogenen Daten durch eine verantwortliche Stelle rechtlich nur dann erlaubt ist, wenn Sie entweder eingewilligt haben oder ein Gesetz es erlaubt.

Ob Ihre personenbezogenen Daten verarbeitet werden dürfen, richtet sich also zunächst danach, ob ein Gesetz dies erlaubt. Die Datenschutzgesetze sind sehr umfangreich, die Erlaubnisnormen zahlreich. Vor allem existieren sogenannte Generalklauseln, die recht weitgehend Datenverarbeitungen erlauben. Oft ausschlaggebend ist eine Interessenabwägung.[1] Es hilft für die konkrete Beurteilung eines datenschutzrechtlichen Sachverhalts also nicht, „freihändig“ – wie die Juristen sagen – mit dem Grundgesetz und dem „Recht auf informationelle Selbstbestimmung“ zu argumentieren. Sie müssen sich konkret mit den speziellen Erlaubnistatbeständen bzw. den Generalklauseln auseinandersetzen.

[1] Zum Beispiel § 28 Absatz 1 Satz 1 Nr. 2 BDSG.

Als Beispiel sei die Generalklausel für die Datenverarbeitung im „nichtöffentlicher Bereich”, also durch Unternehmen, genannt: „Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig,
1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,
2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder
3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.“ (§ 28 Absatz 1 Satz 1 BDSG)

Sie sind gefragt

Sofern nicht ein Gesetz die Verarbeitung erlaubt, muss die „verantwortliche Stelle“ Sie also vor der Verwendung ihrer persönlichen Daten um Ihre Einwilligung bitten. Dies ist auch dann der Fall, wenn Ihre Daten an Dritte weitergegeben werden sollen. Die Einwilligung muss informiert und ausdrücklich erfolgen, regelmäßig sogar in Schriftform.[1] Dies kann auch für Sie lästig sein, wenn Sie zum Beispiel am Telefon einen Vertrag mit Datenverarbeitungsklausel abschließen wollen. Für den Internetbereich bestehen Erleichterungen hinsichtlich der Form. Manchmal führt das Einwilligungserfordernis zu vielen Seiten an Kleingedrucktem. Für Werbung gibt es keinen umfassenden Einwilligungsvorbehalt. Für alle Werbung außer Briefwerbung ist gleichwohl eine Einwilligung vorgeschrieben, die allerdings nicht schriftlich erfolgen muss.[2] Für E-Mail-Werbung gilt, dass Unternehmen ihre eigenen Kunden auch ohne deren ausdrückliche Einwilligung für eigene verwandte Produkte ansprechen dürfen.[3] Stets aber besteht die Möglichkeit für Sie, zukünftiger Werbung zu widersprechen.[4]

„Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.“ (§ 4 a Absatz 1 Sätze 3 und 4 BDSG)

[1] § 4a BDSG.
[2] § 7 Absatz 2 UWG.
[3] § 7 Absatz 3 UWG.
[4] § 28 Absatz 4 BDSG.

LESEN SIE DAS KLEINGEDRUCKTE

Im Netz finden Sie zahlreiche Informationen zum Thema Datenschutz. Die wichtigsten Links haben wir am Ende dieser Broschüre für Sie zusammengestellt.

Hat man bei seiner Gesetzesrecherche dann die einschlägigen Paragraphen gefunden, wird es einfacher. Die Gesetzesvorschriften sind zwar meist in nüchternem Juristendeutsch geschrieben, aber durchaus allgemeinverständlich. Probleme tauchen auf, wenn Begriffe interpretationsbedürftig sind, wie bei den Formulierungen „berechtigte Interessen“ oder „schutzwürdige Belange“.

Neben die Gesetzeslage tritt häufig auch noch das, was zwischen Betroffenem und Verarbeiter vereinbart worden ist. Denn nach der (formellen) Grundregel des Datenschutzes, dem „Verbot mit Erlaubnisvorbehalt“, steht als Erlaubnistatbestand neben dem Gesetz gleichberechtigt die Einwilligung. Und eine solche Einwilligung kann zum Beispiel auch beim Akzeptieren der Allgemeinen Geschäftsbedingungen (AGB) gegeben werden. Bevor man also mit dem Gesetz in der Hand aufgebracht zum Verarbeiter stürmt, sollte man genau das berühmte „Kleingedruckte“ lesen, das man abgenickt und weggeklickt hat. Allerdings ist nicht jede AGB-Klausel auch nach deutschem Recht wirksam, vor allem nicht bloße Übersetzungen angelsächsischer Vertragstexte. In Beschäftigungsverhältnissen kommt noch hinzu, dass – gewissermaßen als Zwischending zwischen Gesetz und Vertrag – auch Betriebsvereinbarungen zu berücksichtigen sind.

ESKALATIONSSTUFEN IM FALLE EINES FALLES

Wenn Sie nach Gesetzes- und Vertragsstudium der Ansicht sind, dass ein Datenschutzverstoß vorliegt, ist es Zeit, aktiv zu werden. Die erste Stufe rechtlichen Vorgehens ist die einfache Bitte an die verantwortliche Stelle, bestimmte Datenverarbeitungen zu unterlassen.

Das wird häufig schon ausreichen, da Unternehmen mit einem guten Ruf an einem harmonischen Verhältnis zu ihren Kunden und einem makellosen Bild in der Öffentlichkeit interessiert sind. Dann können Sie den Verarbeiter um Löschung bitten, also die eingeräumten Widerspruchsrechte ausüben[1] oder Berichtigungs- und Löschungsansprüche[2] geltend machen.

WENN KLAGEN, DANN RICHTIG

Wenn die „verantwortliche Stelle“ auf den Wunsch nach Unterlassung, Berichtigung, Löschung oder Auskunft nicht eingeht, müssen Sie rechtlich tätig werden. Das Instrument hierfür ist die gerichtliche Klage. Wenn Sie es mit einer Behörde, einer „öffentlichen Stelle“, zu tun haben, können Sie statt einer Klage auch eine Dienst-, Fach- oder Rechtsaufsichtsbeschwerde einlegen. Gerichtsverfahren sind in Deutschland im Vergleich zum Ausland recht günstig. Sie sind gleichwohl stets mit Zeitaufwand verbunden und für juristisch Unerfahrene auch nervenaufreibend. Ein Rechtsanwalt gibt oft gute und manchmal notwendige Hilfestellung, kostet aber Geld. Um das zuständige Gericht und die einschlägige Verfahrensart zu finden, ist ein Rechtsanwalt meist unentbehrlich. Es müssen allerdings stets die Fristen im Auge behalten werden. Wer zu spät kommt, wird nicht nur von der Geschichte bestraft, sondern auch vor Gericht nicht mehr gehört. Auch hier hilft ein Anwalt; als Faustregel kann aber gelten, dass keine dafür relevante Frist kürzer als einen Monat ist.

Es hat sich in vielen Fällen gezeigt, dass eine entsprechende Bitte wesentlich eher zum Erfolg führt, wenn man das Geld für eine Briefmarke investiert, also ein Schreiben mit Papier und Tinte aufsetzt. Dabei sollte man auch bedenken, welchen (zeitlichen) Aufwand man bereits für die Ergründung der Sach- und Rechtslage betrieben hat, so dass der zusätzliche Centbetrag kaum noch ergänzend ins Gewicht fällt.

[1] Insb. der Werbewiderspruch nach § 28 Absatz 4 BDSG.
[2] § 20, § 35 BDSG.

Nicht alle Rechtsanwälte sind gleichermaßen auf das Datenschutzrecht spezialisiert. Zwar kann und darf jeder Anwalt ein Datenschutzmandat übernehmen. Einen fachlich passenden Rechtsanwalt findet man unter www.anwaltauskunft.de/anwaltssuche, einem (nichtamtlichen) Suchdienst des Deutschen Anwaltvereins. Empfehlungen oder eine eigene Internetrecherche sind dabei hilfreich.

HILFE VON DATENSCHUTZINSTITUTIONEN

Oft werden Datenschutzansprüche nicht geltend gemacht, weil sie für den Einzelnen nicht so störend sind, dass sich ein Vorgehen wirtschaftlich oder emotional lohnt. Dies ist die zuvor bereits erwähnte „rationale Apathie". Ebenfalls problematisch für die individuelle Durchsetzung des Datenschutzes ist der Umstand, dass ein Eingriff nicht fühlbar ist und deshalb oft schwer und erst verzögert bemerkt werden kann. Dem versucht das Datenschutzrecht entgegenzuwirken, zum Beispiel durch die bereits beschriebenen umfangreichen Informierungs- und Transparenzpflichten der verantwortlichen Stelle gegenüber dem Betroffenen sowie durch institutionelle Hilfestellung bei der Durchsetzung datenschutzrechtlicher Ansprüche. Wegen unerwünschter Werbepost wird kaum jemand den Gang zum Gericht unternehmen, vielleicht aber einen Datenschutzbeauftragten anrufen.

BETRIEBLICHE UND BEHÖRDLICHE BEAUFTRAGTE FÜR DEN DATENSCHUTZ

Erste Ansprechpartner für Sie sind die betrieblichen und behördlichen Beauftragten für den Datenschutz (bDSB).[1] Sie sind einerseits als Teil der verantwortlichen Stelle mit den Umständen der Datenverarbeitung vertraut. Andererseits sind sie in ihrer Funktion unabhängig, so dass sie auch Anlaufstelle für Beschwerden sein können.

[1] § 4f BDSG.

DIE DATENSCHUTZBEAUFTRAGTEN

Die Datenschutzbehörden sind eine weitere Anlaufstelle für Sie. In allen Bundesländern (bis auf Bayern) sind die Landesdatenschutzbeauftragten für die Datenschutzkontrolle der Verwaltung und für die Datenschutzaufsicht über die Wirtschaft[1] zuständig. Diese können den Datenschutz gegenüber Behörden durch Beanstandungen[2] und gegenüber Unternehmen mit Verfügungen[3] und Bußgeldern[4] durchsetzen. Ein Anspruch auf das Tätigwerden der staatlichen Datenschutzkontrollstellen besteht aber nicht.

WENN ZWEI SICH STREITEN, HILFT OFT EIN DRITTER

Bei Datenschutzverstößen durch Unternehmen können Sie auch das Wettbewerbsrecht nutzen, um die Hilfe Dritter zu aktivieren. Denn ein Datenschutzverstoß kann zugleich eine unlautere Wettbewerbshandlung sein, die es den Verbraucherschutzverbänden und vor allem Konkurrenten ermöglicht, den Datenschutzverletzer abzumahnen. Allerdings können Sie hier ein Vorgehen lediglich anregen. Sie haben keinen Anspruch auf ein Einschreiten.

DATENSCHUTZ – ES LIEGT AN IHNEN

Abschließend lässt sich sagen, dass Sie in Sachen Datenschutz mehr Rechtsschutzmöglichkeiten haben, als Sie vielleicht denken. Die Datenverarbeitung setzt entweder Ihre informierte und bewusste Einwilligung voraus oder das Gesetz lässt sie zu. Regelmäßig muss der Verarbeiter Sie beizeiten informieren. Schwarze Schafe können Sie mit Ihrem Auskunftsrecht aufspüren. Um Ihnen die Durchsetzung Ihrer Rechte etwas leichter zu machen, haben wir im Folgenden wichtige Internetquellen zum Datenschutz zusammengestellt.

[1] § 38 Absatz 1 BDSG.
[2] Vgl. § 25 BDSG.
[3] § 38 Absatz 5 BDSG.
[4] § 41 BDSG.

Die Adressen der Datenschutzbehörden finden Sie unter www.datenschutz.de/institutionen/adressen.

Zuständig ist – faustregelhaft – die Behörde, in deren Bundesland der Verarbeiter, die „verantwortliche Stelle", ihren (Geschäfts- bzw. Dienst-) Sitz hat. Für Telekommunikations- und Postunternehmen ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) zuständig. Eine nicht zuständige Behörde wird aber allgemein ein Anliegen an die zuständige weiterleiten, oder zumindest einen entsprechenden Hinweis geben.

Die Adressen der (allgemeinen) Verbraucherschutzzentralen finden Sie unter www.verbraucherzentrale.de.

DATENSCHUTZINFORMATIONEN IM INTERNET

Gemeinsames Portal der Datenschutzbeauftragten:
www.datenschutz.de

Adressen der Datenschutzbehörden:
www.datenschutz.de/institutionen/adressen

Angebot der Stiftung Datenschutz:
www.stiftungdatenschutz.org

Angebot der Bundeszentrale für politische Bildung:
www.bpb.de

Nichtamtlicher Suchdienst des Deutschen Anwaltereins:
www.anwaltauskunft.de/anwaltssuche

Adressen der allgemeinen Verbraucherzentralen:
www.verbraucherzentrale.de

GLOSSAR

AGB: Allgemeinen Geschäftsbedingungen
Das bekannte „Kleingedruckte". Wenn es von einer Vertragspartei einseitig und nicht veränderbar vorgegeben wird, unterliegt es einer verschärften gerichtlichen Kontrolle, ob es nicht unangemessen ist.

bDSB: betrieblicher und behördlicher Datenschutzbeauftragter
Jede Behörde und jedes Unternehmen (abgesehen von Kleinbetrieben) muss eine Person zum „Beauftragten für den Datenschutz" machen. Diese bleibt Teil der Organisation des Verarbeiters, ist aber unabhängig und damit prädestiniert, Konflikte zwischen einem Betroffenen und der verantwortlichen Stelle zu klären.

BDSG: Bundesdatenschutzgesetz
Das Grund-Gesetz des Datenschutzes in Deutschland. Enthält in rechtstechnisch-trockener Sprache die Grundregeln für die Verarbeitung personenbezogener Daten. Viele Datenschutzregeln finden sich aber auch in weiteren Rechtsakten, wie von den Bundesländern oder der Europäischen Union.

BNDG: Gesetz über den Bundesnachrichtendienst
Das BNDG ist das Gesetz über den deutschen Auslandsgeheimdienst. Dessen Aufgaben entsprechen denen der US-amerikanischen NSA (National Security Agency), wenngleich die Befugnisse und wohl auch die technischen Möglichkeiten beschränkter sind.

BVerfSchG: Bundesverfassungsschutzgesetz
Das BVerfSchG regelt die Tätigkeit des Inlandsgeheimdienstes des Bundes; vergleichbare Regelungen gibt es auch in allen Bundesländern. Die Ausforschungsbefugnisse gehen weiter als die der Strafverfolger. Im Gegenzug darf der Verfassungsschutz keine Festnahmen usw. anordnen.

MADG: Gesetz über den Militärischen Abschirmdienst
Das MADG gilt für den deutschen Militärgeheimdienst und hat in der zivilen Praxis deshalb wenig Bedeutung.

StPO: Strafprozessordnung
Die Strafprozessordnung enthält die Regelungen, nach denen Straftaten aufgeklärt werden. Strafverfolgung ist immer mit Eingriffen in Datenschutzrechte verbunden, weshalb die Befugnisse der Sicherheitsbehörden darin inzwischen detailliert beschrieben sind.

TKG: Telekommunikationsgesetz
Der Datenschutz bei der Telekommunikation (Telefon, Fax, Internet) steht nicht im BDSG, sondern in einem Abschnitt des TKG (§§ 88–115). Dieser Abschnitt enthält aber nicht nur Datenschutzvorschriften, sondern zum Beispiel auch die Abhörbefugnisse der Sicherheitsbehörden.

TMG: Telemediengesetz
Der Datenschutz bei der Nutzung von Internetdiensten (Suchmaschinen, soziale Netzwerke, Cloud-Speicher usw.) ist in einem Abschnitt des TMG geregelt (§§ 11–15a). Das TMG enthält neben Internetdatenschutzrichtlinien u. a. auch die Regeln der Provider-Haftung.

UWG: Gesetz gegen den unlauteren Wettbewerb
Das UWG ist das Gesetz über das Auftreten von Unternehmen auf dem Markt, ihren Umgang miteinander und mit den Kunden. Es verbietet unlauteres Handeln, wozu auch der Verstoß gegen Gesetze über den Datenschutz gehört. In praktischer Hinsicht wichtig ist bei dem Gesetz die sogenannte Abmahnung, durch die Verstöße innerhalb von Tagen, teilweise von Stunden beantwortet werden können.

Stiftung Datenschutz
Karl-Rothe-Straße 10–14
04105 Leipzig
Telefon 0341/5861 555-0
Telefax 0341/5861 555-9
mail@stiftungdatenschutz.org
www.stiftungdatenschutz.org

STIFTUNG
DATENSCHUTZ