Betroffen von Datenschutzverstößen – Was kann ich tun?

Handlungsoptionen und Erfolgsaussichten

Stand: 20.06.2022

Ute Bernhardt
bernhardt@netzwerk-datenschutzexpertise.de
Ingo Ruhmann
ruhmann@netzwerk-datenschutzexpertise.de
beide: Elchdamm 56a, 13503 Berlin
Karin Schuler
schuler@netzwerk-datenschutz-expertise.de
Kronprinzenstraße 76, 53173 Bonn
Thilo Weichert
weichert@netzwerk-datenschutz-expertise.de
Waisenhofstraße 41, 24103 Kiel
www.netzwerk-datenschutzexpertise.de

Inhalt

Identitätsklau, Werbe-Cookies ohne Einwilligung, Abgreifen von Fotos im Internet, Diffamierung in sog. sozialen Netzwerken, Gesundheitsdaten in der Personalverwaltung, fremde Videoüberwachung im eigenen Garten … Werden derartige, oft im Verborgenen praktizierte Verstöße gegen den Datenschutz den Betroffenen bekannt, stellt sich für diese die Frage: „Was kann ich dagegen tun?“ Diese einfache Frage stößt auf eine komplexe Realität: Unklar ist oft, welche Technik genutzt wird, wer den Angriff veranlasst hat und wer dafür verantwortlich ist, wer hiergegen wirksam vorgehen könnte und tatsächlich kann, welche Möglichkeiten rechtlich und welche realistischerweise bestehen.

1 Einleitung

1.1 Die geltenden Regelungen

Deutschland und die Mitgliedsstaaten der Europäischen Union (EU) sind demokratische Rechtsstaaten, die Grundrechte gewährleisten. Es gilt das in Art. 8 der europäischen Grundrechte-Charta garantierte Recht auf Datenschutz. Es gilt zudem die europäische Datenschutz-Grundverordnung (DSGVO), die eine Vielzahl von sog. Betroffenenrechten regeln: allen voran das Recht auf Auskunft (Art. 15 DSGVO), zudem ein Recht auf Löschung, sogar „auf Vergessenwerden“ (Art. 17 DSGVO), ein Recht auf Datenberichtigung (Art. 16 DSGVO), ein Recht auf Datensperrung, oder wie es in Art. 18 DSGVO heißt, „auf Einschränkung der Verarbeitung“. Betroffene müssen über die sie betreffende Datenverarbeitung informiert werden (Art. 13, 14 DSGVO). Sie können mit persönlichen Gründen einer Datenverarbeitung widersprechen (Art. 21 DSGVO). Im Fall eines Verstoßes haben sie einen Anspruch auf Entschädigung, auf materiellen oder immateriellen Schadenersatz (Art. 82 DSGVO). Zivilrechtlich bestehen Ansprüche auf Unterlassung und Beseitigung von unzulässigen informationellen Angriffen (§ 823 i.V.m. § 1004 BGB analog). Und um das alles durchzusetzen, garantiert die DSGVO ein Recht auf Beschwerde bei einer Aufsichtsbehörde (Art. 77), ein Recht auf wirksamen gerichtlichen Rechtsschutz gegen Verantwortliche oder Auftragsverarbeiter (Art. 79) und sogar ein Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde (Art. 78).

1.2 Die gelebte Praxis

Das hört sich alles gut an. In der Realität kann sich aber schnell Ernüchterung einstellen, wenn von den gesetzlichen Versprechungen in Wirklichkeit wenig und manchmal gar nichts übrig bleibt. Dass Gesetze nicht zu 100 Prozent durchgesetzt werden, ist in einem freiheitlichen Staat normal: Es gibt nicht nur gesetzestreue Bürgerinnen und Bürger und erst recht nicht nur gesetzestreue Unternehmen. Und die totale Durchsetzung von Gesetzen würde eine Totalkontrolle nötig machen. Deshalb sind Abstriche bei den Erwartungen an die gesetzliche Ordnung zu machen. Dabei wäre es aber wünschenswert, dass schwere Verletzung eher schneller und nachhaltiger verfolgt und sanktioniert werden als unbedeutende Datenschutzverstöße.

Doch auch das ist nicht Realität: Es ist oft gerade umgekehrt. Einige Gründe dafür liegen auf der Hand: Die zuständigen Aufsichtsbehörden sind schlecht ausgestattet und haben viel zu tun. Das Bewusstsein über die Notwendigkeiten beim Datenschutz fehlt bei vielen Menschen und Institutionen. Manche halten nichts vom Datenschutz (der Anderen) und sehen sich deshalb auch nicht veranlasst, sich an die

Gesetze zu halten. Es gibt noch einen weiteren Grund für die Vollzugsdefizite beim Datenschutz: Für viele Unternehmen ist es profitabel, unter Missachtung des Datenschutzes ihre Geschäfte zu machen; ihr Geschäftsmodell beruht darauf, dass sie unter Verletzung von Gesetzen Daten sammeln und nutzen und dabei gewaltige Profite machen, während die Gefahr, dafür sanktioniert zu werden, immer noch gering ist.

1.3 Überblick

Umso wichtiger ist es, dass Betroffene darauf Einfluss nehmen können, dass Ihre Datenschutzrechte beachtet werden. Im Folgenden werden die Möglichkeiten dargestellt und, welche Erfolgschancen damit einhergehen. Anspruch und Wirklichkeit sind auch bei der Wahrnehmung der Betroffenenrechte nicht identisch. Konkret geht es insbesondere um folgende Mechanismen:

- Wahrnehmung der eigenen Rechte direkt gegenüber dem Verantwortlichen und dessen Datenschutzbeauftragten
- Beschwerde bei den Datenschutzaufsichtsbehörden
- Einschaltung von Verbraucherzentralen
- Gang in die Öffentlichkeit.

Bei allen o.g. Aktivitäten muss der Betroffene nicht persönlich tätig werden, sondern kann sich durch eine andere Person vertreten lassen. Wenn hierbei Rechtswirkungen ausgelöst werden sollen, ist es im Fall der Vertretung, z.B. durch einen Anwalt, nötig, dass im Zweifelsfall eine wirksame Vertretungsvollmacht vorgelegt wird.

2 Geltendmachung der Betroffenenrechte beim Verantwortlichen

Es ist sinnvoll, bevor weitere Schritte eingeleitet werden, sich zunächst an die Daten verarbeitende, also die verantwortliche Stelle zu wenden. Das ist die, welche die Daten erhebt und weiterverarbeitet, also z.B. das Handelsunternehmen, der Webseitenbetreiber, der Arbeitgeber oder die Behörde. Handelt ein Auftragsverarbeiter, der für einen Verantwortlichen tätig wird, so kann man sich auch direkt an diesen werden. Um die korrekte Adresse herauszubekommen, gibt es im Internet die Impressumspflicht (§§ 5, 6 Telemediengesetz – TMG). Dort müssen auf der Startseite im Web oder zumindest mit einem weiteren Klick der Name, die Adresse und eine elektronische Kontaktangabe aufgeführt werden.

2.1 Datenschutzbeauftragter

Zumeist unter der Rubrik „Datenschutz“ (und dort leider zumeist erst ganz am Ende) finden sich im Internet Kontaktangaben zum betrieblichen Datenschutzbeauftragten, die der Verantwortliche nach Art. 37 Abs. 7 DSGVO zu veröffentlichen verpflichtet ist. Art. 38 Abs. 4 DSGVO regelt, dass Betroffene sich zur Wahrnehmung ihrer Rechte an den Datenschutzbeauftragten wenden können. Es gibt interne wie externe Datenschutzbeauftragte, also solche in der Stelle selbst, und solche, die selbständig tätig sind, etwa Rechtsanwälte, spezialisierte Datenschutzfachleute oder -firmen.

Man muss sich als Betroffener mit einer Beschwerde nicht an den Datenschutzbeauftragten wenden; Adressat kann auch die Stelle generell oder und deren Leitung sein. Ist dort nicht bekannt, wie mit einer Datenschutzanfrage umzugehen ist; dann liegt es nahe, den insofern ausgebildeten Datenschutzbeauftragten einzuschalten.

2.2 Anspruch auf Auskunft u.a.

Ist unklar, welche Daten bei der Stelle für welche Zweck und nach welcher Rechtsgrundlage verarbeitet werden, woher die Daten stammen und an wen sie weitergegeben werden, dann empfiehlt sich die Inanspruchnahme des Auskunftsrechts gegenüber der Stelle (Art. 15 DSGVO). Eine Begründung hierfür ist nicht nötig. Um Ausflüchte der Stelle zu vermeiden, ist es sinnvoll, den Anlass des Auskunftsersuchens darzustellen. Hat der Verantwortliche Zweifel an der Identität des Betroffenen, so kann er deren Glaubhaftmachung einfordern. Ein bestimmtes Verfahren, z.B. durch Vorlage eines Personalausweises oder Übersendung einer Kopie, kann dabei nicht vorgegeben werden, doch sollte man sich an entsprechendes Vorschlägen orientieren.

Das Ersuchen kann analog oder digital erfolgen und sollte eine Fristsetzung enthalten (z.B. 2 Wochen). Nach erfolglosem Ablauf der Frist sollte zeitnah die Auskunftserteilung angemahnt werden. Erfahrungsgemäß sind erste Antworten hinhaltend („Bitte um etwas Geduld“) oder ausweichend (z.B. „alle Daten, die im Rahmen des Vertragsverhältnisses nötig sind“ oder „alle Daten, die Sie angegeben haben“). Solche Antworten sind ungenügend. Es muss auf Nachfrage präzise angegeben werden, welche konkreten Daten vorliegen und verarbeitet werden. Bleibt die Auskunft aus oder ist sie unzulänglich, so ist das ein Verstoß gegen Art. 15 DSGVO, der von der Aufsichtsbehörde sanktioniert werden kann (s.u. 3).

Analog zum Vorgehen zwecks Erlangung einer Auskunft kann bei der Umsetzung der anderen Betroffenenrechte (Löschung, Berichtigung, Verarbeitungsbeschränkung, Widerspruch, Schadenersatz, Unterlassung, Beseitigung) vorgegangen werden (s.o. 1.1).

Die Erfahrung lehrt, dass Verantwortliche auf eine Betroffenenanfrage oder -beschwerde zunächst nicht adäquat und rechtskonform antworten, jedenfalls dann nicht, wenn sie z.B. einen Rechtsverstoß verbergen wollen. In solchen Fällen ist es sinnvoll, mit Fristsetzung nochmals nachzuhaken, bevor andere und weitere Schritte eingeleitet werden. Alle weiteren Maßnahmen sind aufwändiger, schwerfälliger und zeitintensiver.

2.3 Klageerhebung

Statt den weiter unten noch beschriebenen Vorgehensweisen besteht bei einer unbefriedigenden (rechtswidrigen) Reaktion oder einer Nichtreaktion der angeschriebenen Stelle die Möglichkeit, gegen den Verantwortlichen direkt Klage zu erheben. Bei Klagen gegen Privatunternehmen ist der Zivilrechtsweg gegeben, Klagen gegen öffentliche Stellen, also gegen Behörden, werden vor dem Verwaltungsgericht verhandelt (Art. 79 DSGVO).

3 Beschwerde bei der Aufsichtsbehörde

Gemäß Art. 77 Abs. 1 DSGVO haben Betroffene „unbeschadet eines anderweitigen … gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres gewöhnlichen Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes“. Ist man von einem Verstoß nicht persönlich betroffen, kann dennoch eine Beschwerde eingereicht werden. Es liegt dann aber im freien Ermessen der Datenschutzaufsichtsbehörde, ob sie tätig wird oder nicht. Es ist – angesichts der hohen Arbeitslast, die bei den meisten Aufsichtsbehörden besteht – eher ungewöhnlich, das eine Aufsichtsbehörde auf eine Beschwerde von Nichtbetroffenen mit Ermittlungen reagiert. Etwas anderes gilt, wenn zum

gleichen Thema viele Beschwerden vorliegen oder es sich nach deren Ansicht um einen so schwerwiegenden Vorwurf handelt, dass sie von Amts wegen tätig wird.

3.1 Zuständige Behörde

Aus Art. 77 Abs. 1 DSGVO geht hervor, dass die Beschwerde bei der Behörde des Wohnsitzes, des Arbeitsplatzes oder der tatsächlichen Datenverarbeitung eingereicht werden kann. Diese Behörde ist dann auch für die Zwischen- und die Endnachricht zuständig (Art. 77 Abs. 2 DSGVO). Bearbeitet wird die Beschwerde aber regelmäßig ausschließlich durch die sog. „federführende Aufsichtsbehörde“, die für die europäische Hauptniederlassung des Unternehmens (vgl. Art. 4 Nr. 16 DSGVO) des Verantwortlichen zuständig ist (Art. 60 DSGVO). Diese federführende Behörde leitet die Ermittlungen und kann sich dabei von anderen Aufsichtsbehörden unterstützen lassen (Art. 61 DSGVO). In jedem Fall muss sie alle „betroffenen Aufsichtsbehörden“ einbeziehen. Dies sind die Aufsichtsbehörden, in deren Gebiet eine Niederlassung des Verantwortlichen besteht oder sich erhebliche Auswirkungen der Verarbeitung zeigen, sowie die, bei denen eine Beschwerde eingereicht wurde (Art. 4 Nr. 22 DSGVO). Die federführende und alle anderen betroffenen Aufsichtsbehörden versuchen, eine einheitliche Entscheidung zu treffen (Art. 62 DSGVO); wenn dies misslingt, wird im Rahmen eines komplizierten Verfahrens eine Mehrheitsentscheidung gesucht (Art. 63 ff. DSGVO).

Der Betroffene hat also die Möglichkeit bei seiner Beschwerde zwischen verschiedenen Aufsichtsbehörden zu wählen. Wenn er die Sprache der federführenden Aufsichtsbehörde im Ausland beherrscht, ist es sinnvoll, die Beschwerde direkt dort einzureichen. Ansonsten ist es naheliegend, die Behörde am Wohnort oder am Arbeitsplatz zu befassen. Da die Kommunikation zwischen den Aufsichtsbehörden zumeist in Englisch erfolgt, ist es auch möglich in dieser Sprache die Beschwerde einzureichen; dies ist bei internationalen Vorgängen bei jeder Aufsichtsbehörde möglich.

Strategische Erwägungen können es sinnvoll sein lassen, zu einem Sachverhalt bei verschiedenen Aufsichtsbehörden Beschwerden zu erheben, insbesondere wenn der federführenden Behörde wenig vertraut wird (was bisher mit berechtigten Gründen immer wieder bei der irischen Aufsicht der Fall ist, die europaweit für viele internationale IT-Konzerne federführend ist, weil deren europäischer Hauptsitz in Irland liegt). Dadurch sind alle Beschwerdeadressaten „betroffene Aufsichtsbehörden“ und haben ein Mitentscheidungsrecht bei der abschließenden Entscheidung. Insbesondere bei internationalen NGO-Kampagnen wird immer gerne zu dem Mittel gegriffen, möglichst viele Behörden einzubeziehen. Dies erhöht den Entscheidungsdruck: damit geht aber auch eine gewisse Verkomplizierung und Verlangsamung des Gesamtverfahrens wegen der nötigen Abstimmungsprozesse einher.

In der Regel besteht in jedem EU-Mitgliedsland eine Aufsichtsbehörde. Rechtlich angegliedert an das EU-Verfahren nach der DSGVO sind einige wenige weitere Staaten im Europäischen Wirtschaftsraum (EWR): Norwegen, Island und Liechtenstein. Die Adressen der europäischen Aufsichtsbehörden finden sich im Internet unter

https://www.bfdi.bund.de/DE/Service/Anschriften/Europa/Europa-node.html.

Für Stellen der Europäischen Union (EU) ist der Europäische Datenschutzbeauftragte zuständig:

https://edps.europa.eu/_de.

Das einzige EU-Mitgliedsland mit einer föderalen Struktur bei der Datenschutzaufsicht ist Deutschland. Hier gilt insofern das Bundesdatenschutzgesetz (BDSG). Für öffentliche Stellen des Bundes ist der Bundesbeauftragte für den Datenschutz zuständig (§ 9 Abs. 1 BDSG), ebenso für die Telekommunikations- und Postunternehmen (§ 29 Abs. 1 TTDSG, § 42 Abs. 3 PostG) sowie in einigen sozialrechtlich dominierten Spezialbereichen (z.B. Jobcenter, § 50 Abs. 2 SGB II, länderübergreifende Gesundheitsforschung, § 287a SGB V). Die Landesbeauftragten für den Datenschutz sind für die öffentlichen Stellen in den Ländern zuständig sowie für die nicht-öffentlichen Unternehmen mit dem Hauptsitz in den jeweiligen Bundesländern (§ 40 Abs. 1 BDSG). In Bayern sind für den öffentlichen und den nicht-öffentlichen Bereich unterschiedliche Aufsichtsbehörden zuständig.

Die Adressen der Aufsichtsbehörden in Deutschland finden sich im Internet unter

https://www.bfdi.bund.de/DE/Service/Anschriften/Laender/Laender-node.html.

Weiter wird die Aufsichtsstruktur in Deutschland dadurch verkompliziert, dass es für die Kirchen und die Rundfunkanstalten eigenständige Aufsichtszuständigkeiten gibt:

https://www.bfdi.bund.de/DE/Service/Anschriften/Kirchen/Kirchen-node.html und

https://www.bfdi.bund.de/DE/Service/Anschriften/Rundfunk/Rundfunk-node.html.

Bei der Rechtsprechungstätigkeit der Gerichte und in den Parlamenten ist nur eine interne Datenschutzaufsicht vorgesehen.

3.2 Begründung der Beschwerde

Formale und inhaltliche Voraussetzungen für Datenschutzbeschwerden gibt es nicht. Doch sollten einige Aspekte beachtet werden: Unabdingbar ist es, wenn man auf eine Beschwerde hin auch eine Antwort bzw. Reaktion erwartet, dass die eigenen Erreichbarkeitsdaten präzise benannt werden, also Name, Adresse, möglichst Telefonnummer und E-Mail-Adresse. Fehlt es an den beiden letztgenannten Angaben, werden Rückfragen der Datenschutzaufsicht erschwert. Auf welche Art die Beschwerde die Aufsicht erreicht, ist unwichtig: Post, Fax, Internetformular, Mail, ja theoretisch sind sogar Telefon, persönliche Beschwerde vor Ort oder SMS möglich.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) stellt im Internet ein Beschwerdeformular zur Verfügung:

https://formulare.bfdi.bund.de/lip/form/display.do?%24context=94BD9CBB5DF91650AA09.

Entsprechendes gilt für fast alle anderen Aufsichtsbehörden.

Es ist sinnvoll, den Beschwerdegrund so präzise wie möglich zu benennen. Alles, was zur Aufklärung einer vermeintlich unzulässigen Datenverarbeitung bekannt ist, sollte gleich beim ersten Anschreiben benannt werden: Name, Adresse, Standortangaben des Verantwortlichen oder Auftragsverarbeiters sind wichtig, um die Zuständigkeit festzustellen. Weiterhin ist es angebracht, präzise Angaben zum Beschwerdegrund zu machen: Angaben zu Ort und Zeit, Umstände und – wenn bekannt – über technische Details. Eine juristische Einordnung ist nicht nötig, aber auch nicht schädlich; sie erleichtert dem Sachbearbeiter die erste Einordnung. Dieser hat aber insofern – davon sollte man zumindest

ausgehen – die nötige Sachkompetenz. Abschließend sollte mitgeteilt werden, was angestrebt wird, z.B. eine Auskunftserteilung, eine Datenlöschung, eine Sanktionierung.

3.3 Verfahren

Das Beschwerdeverfahren bei der Datenschutzaufsicht ist für die Betroffenen kostenfrei.

Für die weitere Bearbeitung sollte die Datenschutzaufsicht wissen, ob gegenüber dem vermeintlichen Verletzer des Datenschutzes der Name der Beschwerde führenden Person bzw. des Betroffenen genannt werden kann. Geht es um einen individuellen Datenschutzverstoß, so geht hieran regelmäßig kein Weg vorbei. Handelt es sich dagegen um systematische und strukturelle Verletzungen des Datenschutzes, ist die Identität der Beschwerdeperson nicht von Bedeutung. Es besteht dann die Möglichkeit und bei Wunsch der Anspruch, gegenüber dem Verletzer anonym zu bleiben. Das kann sogar wichtig sein, wenn es sich bei dem Verantwortlichen z.B. um den eigenen Arbeitgeber handelt und man von diesem Ärger befürchtet, wenn dieser von dem Urheber der Datenschutzbeschwerde erfährt. Aber auch bei einem Arzt oder Krankenhaus kann die Befürchtung bestehen, nicht mehr oder nicht so gut behandelt zu werden, oder bei einem Handelsgeschäft, nicht mehr bedient oder beliefert zu werden. Besteht man als Beschwerdeführer auf einer anonymen Bearbeitung, so darf die Aufsicht gegenüber dem Verantwortlichen die Identität des Beschwerdeführers nicht offenlegen.

Auf eine Beschwerde hin erhält man regelmäßig zunächst eine Eingangsbestätigung mit einem Aktenzeichen und evtl. weitere Informationen zum Fortgang der Untersuchung. Diese Untersuchung beschränkt sich oft darauf, dass die Stelle, gegen die sich die Beschwerde richtet, um eine Stellungnahme gebeten wird. Die Erwartung, dass die Behörde unangekündigt vor Ort eine Prüfung vornimmt, ist zumeist unrealistisch. Derartiges ist aber rechtlich möglich und geschieht in Ausnahmefällen, etwa wenn es sich um einen gravierenden und systematischen Verstoß handeln könnte, den die Stelle – z.B. durch eine Datenlöschung – evtl. zu vertuschen versucht. Der ersten Stellungnahme folgt zumeist ein weiterer Austausch zwischen verarbeitender Stelle und Datenschutzaufsicht, regelmäßig unter Einbeziehung des Datenschutzbeauftragten der Stelle, evtl. auch der IT-Administration, der Stellenleitung oder einer anwaltlichen Vertretung der Stelle. Dieser Austausch – der nicht selten ein unergiebiges Ping-Pong ist, bei dem die Stelle abwiegelt, lügt oder gar zum Gegenangriff geht – verliert sich leider selbst in manch gut begründeten Fällen im Nirgendwo.

Immer wieder bleibt es dann für den Beschwerdeführer bei der Eingangsbestätigung: Die Aufsichtsbehörden arbeiten oft am Limit und sind oft mit den verfügbaren Kapazitäten nicht in der Lage, allen Beschwerden nachzugehen. Es ist leider auch nicht selten, dass man einen abwiegelnden Bescheid erhält, der den möglicherweise falschen Darstellungen des vermeintlichen Verletzers ohne Weiteres Glauben schenkt. In solchen Fällen geht kein Weg daran vorbei, falsche Behauptungen richtig zu stellen und – wenn möglich – mit Beweisen zu bekräftigen.

Wird von der Aufsicht ein Datenschutzverstoß festgestellt, so sollte auch eine Sanktion erfolgen. Die möglichen Sanktionen sind in Art. 58 Abs. 2 und Art. 83 DSGVO beschrieben. Diese beginnen mit einer Verwarnung und gehen bis zur Untersagung des Systembetriebs oder bis zu einem Bußgeld in Höhe von 4% des weltweiten Jahresumsatzes eines Unternehmens (Art. 83 Abs. 4, 5 DSGVO). Möglich ist zudem ein Strafantrag (§ 42 Abs. 2 BDSG, s.u. 5.1). Die Herrschaft über ein auf einen Strafantrag oder eine Strafanzeige ausgelöstes Ermittlungsverfahren liegt nicht mehr bei der Datenschutzaufsicht, die dann nur noch zuliefert, sondern bei der Staatsanwaltschaft. Es ist auch möglich, dass die

Öffentlichkeit, z.B. über eine Presseerklärung der Aufsichtsbehörde, von einem Verstoß informiert wird.

Im Fall von berechtigten Beschwerden kann eine Bearbeitung lange, ja Jahre, dauern. Ob es zu einer Sanktion kommt, hängt von vielen Aspekten ab: Der Verstoß muss lückenlos nachgewiesen werden können. Anwaltlich vertretene Stellen wehren sich zumeist mit allen rechtlichen Mitteln gegen Sanktionen. Manche Aufsichtsbehörde scheut – schon wegen des Aufwands – die gerichtliche Auseinandersetzung mit dem Datenschutzverletzer.

Der Beschwerdeführer sollte jeweils über den Stand des Verfahrens und letztlich über das Ergebnis der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs informiert werden (Art. 77 Abs. 2 DSGVO).

3.4 Rechtsschutz

Der Betroffene kann gegen ihn betreffende (Abschluss-)Entscheidungen der Aufsichtsbehörde gerichtlich vorgehen (Art. 78 DSGVO). Mit einer Untätigkeitsklage kann allenfalls erreicht werden, dass eine eingeschlafene Ermittlung wieder lebendig gemacht wird. Eine Klage gegen einen ablehnenden Bescheid der Aufsicht kann dagegen äußerst effektiv sein. Dabei wird nicht nur die Richtigkeit der Verwaltungsentscheidung überprüft, sondern – inzident – ob ein Datenschutzverstoß vorlag. Da dies die verarbeitende Stelle betrifft, wird diese regelmäßig in solchen Verfahren beigeladen, so dass das Verfahren vor dem Verwaltungsgericht zugleich auch Wirkung gegenüber dem möglichen Datenschutzverletzer hat.

4 Einschaltung des Verbraucherschutzes

Schon seit vielen Jahren besteht die Möglichkeit, sich mit einem Datenschutzanliegen auch an eine Verbraucherschutzorganisation, also z.B. eine Verbraucherzentrale, zu wenden und sich dort beraten und evtl. gar vertreten zu lassen. Zunächst stand dabei die Nutzung rechtswidriger allgemeiner Geschäftsbedingungen (AGB) zur Datenverarbeitung im Vordergrund (§§ 305 ff BGB). Seit 2016 wurde eine Regelung im Unterlassungsklagegesetz (§ 2 Abs. 2 Nr. 11 UKlaG) eingeführt, wonach Verbraucherorganisationen im Wege der Unterlassungsklage gegen materiell-rechtliche Datenschutzverstöße vorgehen können. Hiervon machen regionale Verbraucherzentralen und bundesweit vor allem der Verbraucherzentrale Bundesverband e.V. (vzbv = der Zusammenschluss der Verbraucherorganisationen) immer wieder Gebrauch. Hierbei geht es dann regelmäßig um schwerwiegende systematische Verstößen von großen Unternehmen mit einer großen Streubreite, insbesondere im Bereich der Internet-Wirtschaft.

Diese Klagemöglichkeit in Form der Verbandsklage ist in Art. 80 Abs. 2 DSGVO ausdrücklich vorgesehen. Solche prominenten Klagen landen immer wieder beim Europäischem Gerichtshof (EuGH), der dann europaweit geltende Grundsatzentscheidungen fällt.

Die Verbraucherzentralen sind aber auch eine geeignete Anlaufstelle für Betroffene zwecks Beratung bei vermuteten Datenschutzverstößen. Sie geben Hinweise, wie man selbst seine Rechte wahrnehmen kann, unterstützen hierbei oder verweisen auf die Beschwerdemöglichkeit bei den Datenschutzaufsichtsbehörden. Die Aufsichtsbehörden arbeiten teilweise mit den regionalen, den

nationalen und den europäischen Verbraucherorganisationen zusammen. Bei Klagen nach dem UKlaG werden die Aufsichtsbehörden oft mit eingebunden (§ 12a UKlaG).

Seit 2018 ist es für Verbraucherschutzorganisationen auch möglich, für eine Vielzahl von Verletzten von Datenschutzverstößen gemäß dem Musterfeststellungsklagegesetz eine gerichtliche Vorklärung von Betroffenenansprüchen durchführen zu lassen. In Art. 80 Abs. 1 DSGVO ist sogar vorgesehen, dass Verbraucherschutzorganisationen umfassend für Geschädigte von Datenschutzverstößen, etwa zwecks Erstreitung von Schadenersatzansprüchen, gerichtlich vorgehen können. Die dafür nötige spezifische gesetzliche Grundlage besteht aber in Deutschland noch nicht; in der EU bereitet man derzeit gerade eine solche, dann europaweit geltende Regelung vor.

5 Weitere Optionen

Neben den oben genannten etablierten Verfahren bestehen in spezifischen Fällen weitere Möglichkeiten, gegen Datenschutzverstöße vorzugehen.

5.1 Strafanzeige

Neben den Sanktionen wegen Datenschutzverstößen durch die Aufsichtsbehörden gibt es auch das Instrument des Strafrechts zur Bestrafung von Verletzungen des Datenschutzes und des allgemeinen Persönlichkeitsrechts. Die Vorschriften dazu finden sich im Strafgesetzbuch (z.B. §§ 201 ff. StGB), in § 42 BDSG sowie evtl. im sog. Nebenstrafrecht (z.B. § 33 KUG). Zuständig für die Verfolgung dieser Straftaten ist die Staatsanwaltschaft sowie – zu deren Unterstützung – die Polizei. Dorthin kann eine Strafanzeige adressiert werden. Bei vielen Datenschutz-Straftatbeständen ist es nötig, dass ein Strafantrag gestellt werden, der vom Betroffenen, also dem Opfer, innerhalt einer Frist von 3 Monaten nach Kenntniserlangung von Tat und Täter eingereicht werden muss (§§ 77, 77b StGB).

Eine Strafanzeige ist nur bei schwerwiegenden Datenschutzdelikten erfolgversprechend. Voraussetzung ist regelmäßig, dass das Delikt vorsätzlich oder gar absichtlich begangen wurde. Es gibt bisher keine Staatsanwaltschaften, die auf Datenschutz spezialisiert sind. Verstöße werden zumeist nicht dem Begriff Internet-Kriminalität (Cybercrime) zugeordnet. Der Polizei und den Staatsanwaltschaften fehlt es regelmäßig an der für eine Verfolgung nötigen technischen und datenschutzrechtlichen Spezialkenntnis, oft leider immer noch auch am nötigen Problembewusstsein. Deshalb werden Anzeigen zumeist an die Datenschutz-Aufsichtsbehörden abgegeben. Dies muss kein Fehler sein: Erweist sich, dass ein Verstoß strafwürdig ist, kann die Aufsichtsbehörde den Fall (wieder) an die Staatsanwaltschaft abgeben. Im Fall einer Sanktionierung sind eine Geld- oder eine Haftstrafe möglich.

5.2 Kammeraufsicht

Erfolgte ein Datenschutzverstoß durch das Mitglied einer Berufskammer, etwa durch einen Arzt oder durch einen Rechtsanwalt, dann kann eine Beschwerde auch an die zuständige Kammer vorgenommen werden wegen der Verletzung einer berufsrechtlichen Verschwiegenheitspflicht. Solche Verschwiegenheitspflichten finden sich (oft zusätzlich zu § 203 Abs. 1 StGB) im Standesrecht. Eingaben bei der Kammer sind aber nur selten erfolgreich: Dort fehlt es leider oft an der Sachkompetenz und am Problembewusstsein. Es ist üblich, dass die Kammern Eingaben an die Datenschutzaufsicht abgeben. Hinzu kommt, dass die Kammern von Kollegen besetzt sind. Die Bereitschaft, einen Kollegen zu sanktionieren, was bis zu einem Berufsverbot gehen kann, ist zumeist äußerst gering.

5.3 Petition

Eine letzte institutionalisierte Beschwerdeform soll zumindest erwähnt werden: die Wahrnehmung des Petitionsrechts, das in Art. 17 GG besteht als Recht, sich mit „Bitten und Beschwerden“ an die Volksvertretung, also an das zuständige Parlament, zu wenden. Zuständig für solche Eingaben ist bei einem Tätigwerden einer Kommune oder einer Landesbehörde der Landtag des jeweiligen Landes, bei einem Tätigwerden einer Stelle des Bundes der Deutsche Bundestag. Beschwerden sind auch wegen Entscheidungen der Datenschutzaufsicht möglich. In den Parlamenten gibt es jeweils einen Petitionsausschuss. Nach Eingang einer Beschwerde wird regelmäßig die kritisierte Behörde um eine Stellungnahme gebeten. Die Antwort wird dann vom Petitionsausschuss behandelt. Es erfolgt daraufhin ein mehrheitlicher Beschluss der Abgeordneten, der aber keinen erzwingenden Charakter hat.

Da auch im Petitionsausschuss zumeist keine Fachkompetenz besteht, verweist dieser bei Datenschutzverstößen zumeist auf die Aufsichtsbehörde und gibt, wenn diese noch nicht eingeschaltet war, den Fall dorthin ab. Der Ausschuss versteht sich als letzter Notanker, wenn alle anderen Abhilfemöglichkeiten, trotz eines berechtigten Anliegens, erfolglos waren. Daher sollte zuvor die Datenschutzaufsicht eingeschaltet worden sein. Handelt es sich um ein systematisches behördliches Verletzen von Datenschutz, kann eine Petition sinnvoll sein, weil dadurch Abgeordnete hierauf aufmerksam gemacht werden.

6 Gang in die Öffentlichkeit

Die schnellste Reaktion auf einen Datenschutzverstoß kann darin bestehen, hierüber die Öffentlichkeit zu informieren. Damit wird der Verstoß zwar nicht abgestellt, doch kann so evtl. ein gewisser Druck auf den Datenschutzverletzer ausgeübt werden. Zudem besteht die Möglichkeit, andere Betroffene zu informieren und zu mobilisieren. Einen Effekt hat dieser Gang in die Öffentlichkeit aber nur, wenn dadurch die Öffentlichkeit auch erreicht wird. Voraussetzung ist dafür, dass der Verstoß eine besondere Schwere hat und Dritte anspricht. Weitere Voraussetzung ist es, dass die Vorwürfe gut begründet sind und erläutert werden. Bei falschen Darstellungen läuft man Gefahr, von der angegriffenen Stelle kostenpflichtig abgemahnt oder gar verklagt zu werden. Anwälte von angegriffenen Firmen haben erfahrungsgemäß keine Skrupel, wenn sie meinen, dass das von ihnen vertretene Unternehmen unberechtigterweise angegriffen wird oder wenn sie glauben, mit einer Unterlassungserklärung selbst berechtigte Kritik zum Schweigen bringen zu können.

Um sich rückzuversichern, ist evtl. die Einbindung von Nichtregierungsorganisationen (NGOs) sinnvoll. Doch auch diese werden einen Datenschutzverstoß nur dann aufgreifen, wenn er eine grundsätzliche oder größere Bedeutung hat. Die NGOs können ihre Veröffentlichungskanäle nutzen, um vor allem ihre Anhänger und auch die Presse zu erreichen.

Eine solche NGO ist z.B. der Digitalcourage e.V., der jährlich schlimme Datenkraken mit den BigBrotherAwards negativ auszeichnet. Bei vor allem technisch bedingten Datenschutzverstößen kann es sinnvoll sein, sich an den Chaos Computer Club (CCC) zu wenden. Bei Verstößen durch öffentliche Stellen, also Behörden wie insbesondere Polizei und Nachrichtendienste, engagiert sich die Gesellschaft für Freiheitsrechte e.V. (GFF) für die Beachtung des Datenschutzrechts und organisiert bzw. unterstützt musterhafte Klagen vor Gericht. Unterstützung ist auch durch die Deutsche Vereinigung für Datenschutz e.V. (DVD) möglich. Über den deutschsprachigen Bereich hinausgehend

engagiert sich NOYB (none of your business) mit Sitz in Wien für den Datenschutz. NOYB versucht durch gerichtliche Musterklagen gegen Datenkraken vorzugehen.

Eine besondere Art des Widerstands gegen systematische Datenschutzverstöße sind über das Internet organisierte Kampagnen. Doch hier sollte man – wie bei allen im Internet durchgeführten Aktionen – darauf achten, dass man sich nicht vor einen falschen Karren spannen lässt: So manche Online-Kampagne nutzt die Empörung über (vermeintliche) Datenschutzverstöße, um ganz andere Ziele als den digitalen Grundrechtsschutz zu verfolgen.

7 Schlussbemerkung

Die Vollzugsdefizite beim Datenschutz sind gewaltig. Dies ist so, seit es Datenschutz gibt. Mit der DSGVO besteht seit 2018 ein rechtlicher Rahmen, mit dem man sich wirksamer zur Wehr setzen kann. Doch für den „Normalbürger“ bleibt der Weg zur Verteidigung seines „Rechts auf informationelle Selbstbestimmung“ schwierig, zumal es sich zumeist um komplexe technische Vorgänge handelt und die Rechtslage unübersichtlich ist. Dann sind Betroffene auf externe qualifizierte oder gar professionelle Hilfe angewiesen. Hierfür gibt es gemäß der DSGVO vorrangig die unabhängigen Datenschutzaufsichtsbehörden. Diese können aber auch nur einen bedingten Schutz gewährleisten, weshalb weitere Instanzen zur Wahrung des Datenschutzes in Betracht kommen: Verbraucherschützer, Nichtregierungsorganisationen, die Medien. Letztlich geht es nicht nur um den individuellen Datenschutz, sondern darum, dass wir in einer freien, d.h. auch möglichst überwachungsfreien Gesellschaft leben, in der wir unsere Grundrechte und Freiheiten selbstbestimmt wahrnehmen können. Die gesellschaftliche Durchsetzung des Datenschutzes bleibt dabei davon abhängig, dass viele Einzelne ihre Rechte in Anspruch nehmen. Es handelt sich hier um einen dauernden, immer wieder neu zu führenden Kampf, weil für Staat und Wirtschaft informationelle Fremdbestimmung von Menschen immer wieder attraktiv erscheint.

Verwendete Abkürzungen

Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
Art.	Artikel
BGB	Bürgerliches Gesetzbuch
d.h.	das heißt
DSGVO	Europäische Datenschutz-Grundverordnung
evtl.	eventuell
GG	Grundgesetz
KUG	Kunsturhebergesetz
SGB	Sozialgesetzbuch
s.o.	siehe oben
sog.	so genannt
StGB	Strafgesetzbuch
s.u.	siehe unten
TMG	Telemediengesetz
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
UKlaG	Unterlassungsklagegesetz
z.B.	zum Beispiel