Datenschutz newsbox

Ausgabe 6 2019

DATAKONTEXT

Editorial

Die DS-GVO ist vor kurzem 365 Tage alt geworden. Das ist zwar eine recht interessante Info, aber auch doch nur eine Randnotiz der letzten Wochen gewesen. Es gibt aber noch weitere Zahlen, über die man ggf. hinweg gelesen hat.

Die Berliner Charité hat bspw. nach eigenen Angaben 15 Mitarbeiter eingestellt, die sich den ganzen lieben Tag mit nichts anderem beschäftigen, als sich um die Datenschutz-Folgeabschätzungen nach Art. 35 DS-GVO zu kümmern, die im Rahmen der Verarbeitung personenbezogener Daten in der Charité so anfallen.

Die IAPP (International Association of Privacy Professionals) hat Datenschutz-Aufsichtsbehörden in Bulgarien, Deutschland, Dänemark, Finnland, Frankreich, Irland, Italien, Niederlande, Spanien, Schweden, Österreich und dem Vereinigten Königreich gefragt und dabei herausgefunden, dass bisher insgesamt rund 500.000 Unternehmen einen Datenschutzbeauftragten ernannt haben. Die Anzahl der Unternehmen mit einem Datenschutzbeauftragten in Deutschland schätzt die IAPP auf rund 200.000.

Die CNIL hat ein Bußgeld von 400.000 € gegen ein Immobilienunternehmen für einen Verstoß gegen Art. 32 DS-GVO erlassen. Die spanische Datenschutzbehörde AEPD wiederum hat den Ausrichter Liga Nacional de Fútbol Profesional (LFP), auch als "La Liga" bekannt mit einem Bußgeld von 250.000 € belegt. Die App der La Liga nahm ohne das Wissen der Nutzer zu den Spielzeiten Umgebungsgeräusche auf. Die versteckte Absicht war, anhand der der Umgebungsgeräusche und der Kombination mit Ortungsdaten unlizenzierte Fußballübertragungen in Gaststätten entlarven zu können.

Der baden-württembergische Landesdatenschutzbeauftragte Stefan Brink wird wahrscheinlich als erster in die DS-GVO-Geschichte eingehen, der ein Bußgeld gegen einen Mitarbeiter einer öffentlichen Stelle verhängt hat. Ein Polizeibeamter missbrauchte seine Dienstzugänge, um an die Daten einer flüchtigen Bekanntschaft zu gelangen. Zweckwidrig rief der Beamte das Kfz-Kennzeichen der Zufallsbekanntschaft ab. Mit den vom Kraftfahrtbundesamt erhaltenen Daten konnte er dann eine Abfrage bei der Bundesnetzagentur durchführen, die dann im Ergebnis sowohl die Festnetz- als auch an die Mobilfunknummer der Bekanntschaft zu Tage brachte. Dieser Datenschutz-Verstoß kostete den Polizisten 1.400 €.

Falls Sie an einem Überblick und weiterer Lektüre der Bußgelder und Sanktionen interessiert sind, die die Datenschutzbehörden in der EU im Rahmen der DS-GVO verhängt haben, kann Ihnen der enforcementtracker ans Herz gelegt werden.

Ihr Levent Ferik

DATAKONTEXT

Impressum

DATAKONTEXT GmbH
Augustinusstraße 9d
50226 Frechen

Tel.: 02234/98 94 9-30
Fax: 02234/98 94 9-32
fachverlag@datakontext.com
www.datakontext.com

Geschäftsführer:
Dr. Karl Ulrich/Hans-Günter Böse
Handelsregister
Amtsgericht Köln HRB 82299

Aufnahme von Stammdaten ins CRM-System

Frage des GDD-Erfa-Kreises Coburg:
Immer häufiger kommt es vor, dass folgende Mails bei uns eintreffen:
"Informationspflicht gemäß Artikel 13 DSGVO
Sehr geehrte Herr XY,
Aufgrund der neuen DS-GVO (*) zur Speicherung personenbezogener Daten, informieren wir Sie hiermit:
dass die Muster GmbH, Dortmund, personenbezogene Daten (Name, Adresse, Telefonnummer, Email-Adresse, Identifikationsnummer) von Ihnen speichert. Zweck der Speicherung ist die Auftragsabwicklung im Rahmen der Wartungs-/Supportverträge im SAP Solution Manager Service Desk, in denen Sie von unserem Auftraggeber benannt worden sind bzw. benannt werden sollen. Diese Daten werden im Rahmen der Auftragsanbahnung und Supportabwicklung/ Vertragserfüllung verarbeitet/gespeichert.
Diese Daten werden nach dem Ablauf der gesetzlich vorgeschriebenen Aufbewahrungsfristen gelöscht. Sie können jederzeit Auskunft über die Sie betreffenden gespeicherten personenbezogenen Daten verlangen. Sie können jederzeit und ohne Angabe von Gründen z.B. per Mail an xxxx@xxx.xx der Verarbeitung/Speicherung Ihrer personenbezogenen Daten widersprechen.
(*) Die Datenschutz-Grundverordnung (DS-GVO) ist eine Verordnung der Europäischen Union und soll die EU-Datenschutzrichtlinie zum 25. Mai 2018 als direkt geltendes Recht in allen Mitgliedsstaaten ablösen. Die EU-DSGVO soll die Regeln für die Verarbeitung von personenbezogenen Daten durch Unternehmen und öffentliche Institutionen EU-weit vereinheitlichen."
Müssen solche Mails als zusätzliche Info an Interessenten/Kunden/Lieferanten verschickt werden, falls die Stammdaten im CRM aufgenommen und gespeichert werden?

Antwort des BayLDA:
Diese Frage betrifft zwei Fragestellungen: Zum einen, ob Bestandskunden informiert werden müssen und zum anderen was unter "Erhebung" in Artt. 13 und 14 DS-GVO zu verstehen ist.
Das WP 260 äußert sich nicht eindeutig zu den Informationspflichten für Bestandskunden, eine Information kann aber sinnvoll sein.
Bezüglich des Erhebens gibt es derzeit im Kreis der deutschen Aufsichtsbehörden Überlegungen, wie dieses zu definieren ist. Man stellt sich die Frage, ob es Fälle gibt, in denen zwar Daten verarbeitet, aber nicht erhoben werden (Stichwort: aufgedrängte Daten) und daher keine Informationspflichten bestehen. Die Ergebnisse dort sind abzuwarten.
Nachdem bei Erhebung grundsätzlich die Pflichten nach Artt. 13 und 14 DS-GVO bestehen, muss die Informationen in geeigneter Weise zur Verfügung gestellt werden. Dies muss nicht mit einer E-Mail passieren. Die zitierte E-Mail enthält nicht alle Angaben nach Art. 13 DS-GVO. Es fehlen als Betroffenenrecht mindestens noch das Beschwerderecht bei einer Aufsichtsbehörde und das Recht auf Berichtigung.

Info-Broschüre der LDI NRW zum Thema Personalausweis und Datenschutz

Die Landesbeauftragte für Datenschutz und Informationsfreiheit NordrheinWestfalen (LDI NRW) hat zu der praxisrelevanten Frage, wer welche Daten aus dem Personalausweises eines Betroffenen notieren oder kopieren oder gar scannen darf, eine aktuelle Orientierungshilfe veröffentlicht. Die Broschüre enthält zahlreiche Fallgestaltungen, die in der Praxis häufig Fragen aufwerfen. Bei Unsicherheiten bezüglich der zulässigen Nutzung von Ausweisen kann die Broschüre ein nützliches Nachschlagewerk sein.

Im Alltag dienen Personalausweise und Reisepässe oft zum Identifizieren gegenüber Behörden, Banken oder etwa Versicherungen. Ausweise enthalten dabei zahlreiche personenbezogene Daten. Hier ist deshalb besondere Sorgfalt angebracht.
Eine kurze Erläuterung der Struktur des Personalausweises und der optionalen Online-Funktion runden die Empfehlungen der LDI NRW ab.

Quelle: LDI NRW

BayLfD veröffentlicht Orientierungshilfe zu Datenpannen

Nach ErwG 85 der DS-GVO kann eine Verletzung des Schutzes personenbezogener Daten – wenn nicht rechtzeitig und angemessen reagiert wird – einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person.
Deshalb soll nach dem Willen des Verordnungsgebers der Verantwortliche, sobald ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die Aufsichtsbehörde von der Verletzung des Schutzes personenbezogener Daten unverzüglich und, falls möglich, binnen höchstens 72 Stunden, nachdem ihm die Verletzung bekannt wurde, unterrichten, es sei denn, der Verantwortliche kann im Einklang mit dem Grundsatz der Rechenschaftspflicht nachweisen, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt.
Auf der Grundlage der bisher gewonnenen Erfahrungen hat der Bayerische Landesbeauftragte für den Datenschutz die Orientierungshilfe "Meldepflicht und Benachrichtigungspflicht des Verantwortlichen" veröffentlicht, die zahlreiche Zweifelsfragen aufgreift und die einschlägigen Vorschriften der Datenschutz-Grundverordnung sowie des bayerischen Landesrechts für die bayerische Verwaltungspraxis umfassend erläutert. Dabei macht die Orientierungshilfe deutlich, dass nicht jeder Verstoß gegen datenschutzrechtliche Vorschriften, sondern nur eine Verletzung der Sicherheit personenbezogener Daten die Melde- und gegebenenfalls die Benachrichtigungspflicht auslöst. Sie gibt ratsuchenden öffentlichen Stellen weiterhin Empfehlungen für eine vereinfachte Risikoanalyse sowie für die Nutzung des mit Geltungsbeginn der Datenschutz-Grundverordnung eingeführten Online-Meldeformulars.
Die neue Orientierungshilfe ist seit auf https://www.datenschutz-bayern.de in der Rubrik "Datenschutzreform 2018" zum kostenfreien Abruf bereitgestellt.

Wissenschaftspreis für Datenschutz und Datensicherheit

In diesem Jahr vergibt die GDD erneut einen Wissenschaftspreis für herausragende wissenschaftliche Arbeiten in den Bereichen Datenschutz und Datensicherheit. Der Preis beträgt 5.000,00 €. Der Preis kann auch zwischen mehreren Arbeiten geteilt werden.
Der Preis soll bevorzugt an Nachwuchswissenschaftler vergeben werden. Es werden fertiggestellte oder in der Fertigstellung befindliche Abschlussarbeiten oder Doktorarbeiten ausgezeichnet. In Betracht kommen neben Arbeiten aus den Rechtswissenschaften, Wirtschaftswissenschaften und der Informatik auch aus anderen Wissenschaftsdisziplinen, die Fragen aus den Bereichen Datenschutz und Datensicherheit behandeln. Voraussetzung für die Vergabe des Wissenschaftspreises ist die Erfüllung der wissenschaftlichen Exzellenzkriterien.
Die Arbeiten müssen mit Befürwortung des betreuenden Hochschullehrers bei der GDD-Geschäftsstelle bis zum 31. Juli 2019 eingereicht werden.
Nähere Informationen zum Wissenschaftspreis stehen als PDF-Datei und Word-Dokumentals Download zur Verfügung.

Veröffentlichung von Kinderfotos nur mit Einverständnis beider Elternteile

Nach einem Urteil des OLG Oldenburg handelt es sich bei der Veröffentlichung eines Kinderfotos um eine Angelegenheit der elterlichen Sorge. Die Regelung stelle eine Angelegenheit erheblicher Bedeutung für das Kind dar.
Das OLG weist in seinem Urteil zunächst darauf hin, dass gemäß § 22 KunstUrhG Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden dürfen. Hierzu zähle auch das Einstellen von Fotos auf einer Internetseite. Sei der Abgebildete minderjährig, bedürfe es zusätzlich der Einwilligung seines gesetzlichen Vertreters. Dies sind im Regelfall gemäß § 1629 BGB die sorgeberechtigten Eltern, so das OLG Oldenburg.

Bei gemeinsamem Sorgerecht ist eine einvernehmliche Einwilligung beider Elternteile notwendig

Sofern ein gemeinsames Sorgerecht bestehe, sei es notwendig, dass eine einvernehmliche Einwilligung beider Elternteile vorliege. In dem streitgegenständlichen Fall waren die Eltern des sechsjährigen Kindes geschieden und die Mutter besaß das Aufenthaltsbestimmungsrecht über die Tochter. Darüber hinaus galt das gemeinsame Sorgerecht. Im Zusammenhang mit der Veröffentlichung des Kinder-Fotos, welches für die Werbung auf der Internetseite des neuen Lebenspartners der Mutter verwendet wurde, sah das Gericht eine hohe Gefährdung des Rechts der Tochter. Bei der Veröffentlichung von Fotos im Internet würden die Fotos einem unbegrenzten Personenkreis zugänglich gemacht.

Quelle: Justizportal Niedersachsen

Videoüberwachung nach BDSG europarechtswidrig

Das Bundesverwaltungsgericht hat in seiner jetzt veröffentlichten Entscheidung vom 27. März 2019 deutlich gemacht, dass die Videoüberwachung durch private Stellen ausschließlich am europäischen Datenschutzrecht zu messen ist. In dem zugrunde liegenden Fall ging es um eine Anordnung der Brandenburgischen Beauftragten für Datenschutz und für das Recht auf Akteneinsicht zur datenschutzkonformen Ausrichtung der Videoüberwachung in einer Zahnarztpraxis.
Nach Auffassung des Bundesverwaltungsgerichts regelt die Europäische Datenschutzgrundverordnung (DS-GVO) die Videoüberwachung durch Private abschließend. Folglich ist die nationale Bestimmung in § 4 Abs. 1 S. 1 BDSG europarechtswidrig und im Ergebnis unanwendbar. Private Videokameras können daher im Ergebnis nur auf der Rechtsgrundlage des Art. 6 Abs. 1 Buchstabe f DS-GVO betrieben werden. Die danach zu erfolgende Güterabwägung ist nicht durch nationales Recht modifizierbar.

Quelle: Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Einwilligungen und Informationspflichten nach DS-GVO

Frage des GDD-Erfa-Kreises Coburg zu Einwilligungen und Informationspflichten:

Das Unternehmen [A] hat seine Kunden bzw. die Ansprechpartner bei Kunden informiert, dass die vorhandenen Daten wie E-Mailadresse (mit Einwilligung) auch für Newslettermarketing benutzt werden. Die Newsletter wurden bisher immer vom Unternehmen A selbst verschickt. Nun beschließt das Unternehmen A, einen (Internet-)Dienstleister [B] zum Versand der Newsletter einzusetzen und gibt die E-Mailadressen der Betroffenen an B weiter (AV-Vertrag liegt vor).

Müssen die Betroffenen nun von dieser Änderung (zukünftige Weitergabe der Daten an Dritte bzw. andere Empfänger) informiert und erneut in Kenntnis gesetzt werden oder reicht die ursprüngliche erste Information bei Erhebung der Einwilligung, als noch kein Dienstleister eingeschaltet wurde?

Antwort des BayLDA:

Um Missverständnissen vorzubeugen: Einwilligungen und Informationspflichten sind zwei unterschiedliche voneinander zu trennende Anforderungen der DS-GVO.

Für die Einschaltung des Dienstleisters, der offenbar eine Auftragsverarbeitung vornimmt, ist keine Einwilligung nötig. Die Verarbeitung hat sich aber seit der Information der betroffenen Personen geändert. Solche nicht nur unwesentlichen Änderungen sind diesen auch transparent zu machen.

Vgl. dazu auch Rn. 29 – 32 des WP 260.

Frage des GDD-Erfa-Kreises Coburg:

Ist es, um den Informationspflichten nach Art. 13 DS-GVO zu genügen, ausreichend, wenn man einen Link in die Signatur jeder versendeten E-Mail aufnimmt? Dieser Link führt zu einer Unterseite auf der Homepage des Versenders, auf der sich die Datenschutzinformationen nach Art. 13 DS-GVO aufgegliedert nach "Bewerber", "Mitarbeiter", "Kunden", "Lieferanten" und "Interessenten" befinden. Ein weiterer Kommentar oder Erläuterung hierzu erfolgt in der E-Mail nicht.

Oder muss zukünftig jeder Betroffene nach Erhebung seiner Daten direkt per E-Mail mit den Informationen des Art. 13 DS-GVO angeschrieben werden? Muss / sollte dies in irgendeiner Form dokumentiert werden?

Antwort des BayLDA:

Siehe dazu auch diese beiden vorherigen Fragen :

Im Rahmen der gestuften Information müsste bei dem Hinweis auf den Link in der ersten Schicht, der Verantwortliche, Zwecke der Verarbeitung und das Bestehen von Rechten erwähnt werden. Der Verantwortliche und die Zweck werden sich meist schon aus dem Schriftverkehr ergeben, sodass hier die Ausnahme in Art. 13 Abs. 4 bzw. Art. 14 Abs. 5 lit. a) DS-GVO greift. Das Bestehen von Rechten müsste in dem Hinweis auf den Link aufgenommen werden.

Dass Informationen nach Art. 13 und 14 zur Verfügung gestellt werden, muss im Rahmen der Rechenschaftspflichten nach Art. 5 Abs. 2 und Art. 24 Abs. 1 DS-GVO nachweisbar sein. Es gibt derzeit noch keine gefestigte Meinung, wie der Nachweis konkret erfolgen muss.

Gutachten zur Umsetzung der DS-GVO

Die grüne Bundestagsfraktion hat ein Gutachten zur Umsetzung der DS-GVO in Auftrag gegeben. Dieses ist Mitte Mai veröffentlicht worden und ist für alle Interessierte zugänglich. Das Gutachten ist von dem ehemaligen Landesbeauftragten für den Datenschutz und die Informationsfreiheit des Landes Berlin, Dr. Alexander Dix, LL.M., sowie dem ehemaligen Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar angefertigt worden.
Beide Gutachter ziehen zum " ersten Geburtstag" nach Wirksamwerden der DS-GVO eine Bilanz und widerlegen in ihrem Gutachter zahlreiche Behauptungen zu den Folgen der DS-GVO. So werden hartnäckige Gerüchte ausgeräumt, wie die Behauptung, dass mit Wirksamwerden der DS-GVO die Verarbeitung personenbezogener Daten nur noch auf eine Einwilligung gestützt werden könne. Außerdem wird dargelegt, dass es weder die befürchtete Welle unzulässiger Abmahnungen gegen Kleinstunternehmen und Vereine, noch die behaupteten Einschränkungen der Allgemeinkommunikation gegeben habe. Der Umstand, dass die DS-GVO bspw. im Hinblick auf Fotografien im öffentlichen Raum zu gewissen Unsicherheiten geführt habe, wird zwar zugestanden, jedoch wieder mit der Begründung relativiert, dass sich die Rechtslage nicht grundlegende geändert habe.
Als weitere Themen adressiert das Gutachten die immer wieder entfachte Diskussion um das Thema, ob der "deutsche Sonderweg" im Hinblick auf den Schwellenwert für die Bedienungspflicht für Datenschutzbeauftragte tatsächlich ein Bürde für Unternehmen ist oder eher ein Segen. Neben anderen Themen gehen die beiden Gutachtet auch auf die ePrivacy-Verordnung als zukünftigen Rechtsrahmen für die Telekommunikation und das Internet ein.

Quelle: Bündnis 90/Die Grünen Bundestagsfraktion

Informationspflichten nach Art. 13 DS-GVO in AGB einbetten

Frage des GDD-Erfa-Kreises Coburg zu Informationspflichten in den AGB:
Wenn ein Vertrag mit einem Verbraucher zustande kommt, könnten dann die Informationspflichten auch in den AGB enthalten sein, sofern auf diese transparent und gesondert hingewiesen wird. Im B2B Bereich denken wir, dass dies nicht möglich ist, da die betroffene Person diese nicht selbst unterschreibt, sondern die Firma. Sieht die Aufsicht dies auch so?

Antwort des BayLDA:
Aus dem Erfordernis des "Zurverfügungstellens" schließen wir, dass die Informationen nicht jeder betroffenen Person aufgedrängt werden müssen. Es reicht, wenn sie die Möglichkeit hat, diese leicht zu finden und zu lesen. Dies muss nachweisbar sein. Es muss aber wohl nicht nachgewiesen werden, dass jeder einzelnen betroffenen Person die Information tatsächlich übergeben wurde. Eine Unterschrift, dass die Information erfolgt ist, ist daher nicht zwingend notwendig. Die Informationen müssen jedoch leicht auffindbar sein. Sie dürfen nicht "versteckt" werden.
Im B2B-Bereich müsste geklärt werden, wie die Information zur Verfügung gestellt werden kann und ob mit den Partnern ggf. vereinbart werden kann, dass diese ihren Mitarbeitern entsprechende Informationen zur Verfügung stellen, sodass Sie sich auf die Ausnahme in Art. 13 Abs. 4 bzw. 14 Abs. 5 lit. a) DS-GVO berufen können.

Der LfDI Mecklenburg-Vorpommern legt seinen Tätigkeitsbericht vor

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, Heinz Müller, hat den Tätigkeitsbericht seiner Behörde für das Jahr 2018 vorgelegt.

DS-GVO macht Arbeit

Die Anwendung der DS-GVO ab dem 25. Mai 2018 führte zu einer breiten Hysterie sowohl im öffentlichen als auch im privaten Sektor. Zwar war die DS-GVO bereits 2016 in ganz Europa in Kraft gesetzt worden. Die zweijährige Übergangszeit blieb jedoch laut Müller weitgehend ungenutzt. So konnte man im Mai 2018 den Eindruck gewinnen, das neue Recht sei über Nacht gekommen. Die Nachfrage nach Information, Schulung und Beratung explodierte geradezu. "Wir haben in zahlreichen Schulungen und Informationsveranstaltungen immer wieder klargestellt, welche Anforderungen wirklich neu sind und welche an bestehendes deutsches Recht anknüpfen, und dadurch zu einer Versachlichung der Debatte beigetragen", sagt Müller rückblickend

Das Beschwerdeaufkommen beim Landesbeauftragten hat sich im Jahr 2018 gegenüber dem Vorjahr verdreifacht. Aber auch neben den zahlreichen Beschwerden ist die Arbeit der Behörde gewachsen. Durch die DS-GVO hat der Landesbeauftragte über 50 neue Aufgaben erhalten. Das stark gestiegene Arbeitsaufkommen muss die Behörde des Landesbeauftragten bisher mit einem unveränderten Personalbestand bewältigen. Im Januar 2018 wurden zwar fünf neue Stellen geschaffen. Die Zahl der Beschäftigten erhöhte sich dadurch jedoch nicht, weil lediglich fünf befristete Arbeitsverhältnisse in feste Arbeitsverhältnisse umgewandelt wurden. "Ich erwarte", sagt Müller, "dass sich die kürzlich von der Landesregierung beschlossene Aussetzung des Personalkonzepts auch auf meine Behörde auswirkt."

Datenschutz im Verein

Vor besondere Herausforderungen stellt die DS-GVO die Vereine. Vereinsvorstände sind größtenteils ehrenamtlich tätig und müssen sich seit Mai 2018 mit Fragen befassen wie: "Brauchen wir einen Datenschutzbeauftragten? Müssen wir von unseren Vereinsmitgliedern Einwilligungen einholen, um deren Daten im Verein verarbeiten zu dürfen? Dürfen wir Fotos vom letzten Fußballturnier auf unsere Homepage stellen?". Für die Vereine hat der Landesbeauftragte daher gemeinsam mit der Ehrenamtsstiftung einen Leitfaden entwickelt, der seit Oktober 2018 kostenlos beim Landesbeauftragten erhältlich ist.

Weiter auf DataAgenda

LfDI BW veröffentlicht Muster für Joint Controllership

Die DS-GVO geht in Art. 26 DS-GVO davon aus, dass mehrere Akteure gemeinsam für Verarbeitungen im Zusammenhang mit personenbezogenen Daten verantwortlich sein können (Joint Controllership).
Gemäß Art. 26 Abs. 1 DS-GVO sind mehrere Stellen "gemeinsam für die Verarbeitung Verantwortliche", wenn sie gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen. Der "Verantwortliche" wird in Art. 4 Nr. 7 DS-GVO definiert. In diesem Sinne bedingt eine gemeinsame Verantwortlichkeit, dass zwei oder mehrere Verantwortliche gemeinsam personenbezogene Daten verarbeiten.
Bislang gab es in nur wenige Veröffentlichungen von Seiten der Aufsichtsbehörden, die sich mit dem Thema der Gemeinsam Verantwortlichen beschäftigen, obwohl die Rechtsfigur der "gemeinsamen Verantwortlichkeit" und die damit verbundene Frage, wie eine solche vertragliche Vereinbarung zwischen den beteiligten Verantwortlichen eigentlich auszugestalten ist, seit Bekanntwerden des Art. 26 DS-GVO bei vielen Verantwortlichen große Fragezeichen auslöste.
Lediglich das Kurzpapier Nr. 16 "Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DS-GVO" der Datenschutzkonferenz unternahm den Versuch den Begriff und die mit dem Thema zusammenhängenden Abgrenzungsfragen aufzuarbeiten. Die noch weiterhin bestehenden Unsicherheiten rund um diese Rechtsfigur versucht nun der LfDI BW auszuräumen und stellt ein Vertragsmuster zur gemeinsamen Verantwortlichkeit nach Artikel 26 DS-GVO zur Verfügung. Dieses Muster wurde auf Grundlage gemeinsamer Überlegungen mit einer Reihe von Unternehmen und öffentlichen Stellen entwickelt.

Zertifizierung zum IT-Grundschutz-Berater

Unternehmen und Behörden, die sich mit Fragen zum Themenkomplex Informationssicherheit beschäftigen möchten, benötigen oftmals externe Unterstützung. Meist fehlt es noch an den notwendigen personellen und zeitlichen Ressourcen, um sich dem Thema intern widmen zu können. Für die fachliche Unterstützung bei dem Aufbau eines Managementsystems zur Informationssicherheit (ISMS) oder einzelner Aspekte werden daher regelmäßig externe Berater beauftragt. Um sichergehen zu können, dass diese die erforderliche Fachkompetenz mitbringen, fordern die Institutionen oft entsprechende Nachweise von den Beratern. Für einen einheitlichen Nachweis von hoher fachlicher Expertise bietet das BSI eine Personenzertifizierung zum IT-Grundschutz-Berater an.
Die zertifizierten IT-Grundschutz-Berater können Behörden und Unternehmen bei der Entwicklung von Sicherheitskonzepten unterstützen oder bei der Einführung eines Managementsystems zur Informationssicherheit begleiten. Im operativen Tagesgeschäft können sie mit den zuständigen Mitarbeitern auf Basis des IT-Grundschutzes Maßnahmen definieren und im Betrieb umsetzen. Zertifizierte IT-Grundschutz-Berater können zudem dabei unterstützen, ein ISO 27001 Audit auf Basis von IT-Grundschutz vorzubereiten.
Das neue Zertifizierungsangebot basiert auf einem zweistufigen Schulungskonzept. Im ersten Schritt kann der Nachweis als IT-Grundschutz-Praktiker abgelegt werden. Nach einer Aufbauschulung erfolgt dann die Personenzertifizierung zum IT-Grundschutz-Berater.

Quelle: Bundesamt für Sicherheit in der Informationstechnik