Datenschutz
newsbox

Ausgabe
8
2018

DATAKONTEXT

Editorial

Nicht nur die Verarbeitung von Daten des Tierhalters, sondern auch die Verarbeitung von Daten des Tieres, ist zumindest dann eine Verarbeitung personenbezogener Daten, wenn die das Tier betreffenden Informationen einen Rückschluss auf natürliche Personen zulassen. Damit ist nachvollziehbar, dass die Ablehnung einer DNA-Datenbank gegen Hundekot wegen Datenschutz-Bedenken nicht ganz so abwegig erscheint, wie auf den ersten Blick.

Und auch sonst stellt sich bei Nachrichten, die Aspekte des Datenschutzes als Verhinderungsgrund darstellen, die Frage: Wurde die Verarbeitung der personenbezogenen Daten wegen des Datenschutzes oder eher Dank des Datenschutzes verhindert und hätte es nicht Wege gegeben, die beabsichtigte Verarbeitung mit verhältnismäßigem Aufwand doch durchzuführen?

Müssen Zeugnisse tatsächlich wegen des Datenschutzes mit der Hand geschrieben werden? Gab es wirklich keine andere Lösung, dem Persönlichkeitsrecht von Vorschulkindern gerecht zu werden, als deren Fotos in den Erinnerungsmappen mit blauer Farbe unkenntlich zu machen oder wurden die Verantwortlichen (wenn überhaupt) in dem Fall nur schlecht beraten?

Es ist davon auszugehen, dass viele der Unsicherheiten und Irritationen der letzten Monate, die die Betroffenen erfahren mussten, nur mit gezielten Informationen wiederaufgearbeitet und entmystifiziert werden können, meint 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

Aus der Reihe: "Die Aufsichtsbehörde antwortet ..."

Aufbewahrung von Bewerbungsunterlagen

Frage des GDD Erfa-Kreises Würzburg:

Wenn man als Unternehmen Bewerbungsunterlagen über eine Leih-/Zeitarbeitsfirma erhält, sind diese Unterlagen dann als Geschäftsbriefe zu bewerten und müssen 5 bzw. 10 Jahre lang aufbewahrt werden? Gibt es eine Differenzierung, ob man den Kandidaten eingestellt hat oder nicht?

Antwort des BayLDA:

Wir sehen Bewerbungsunterlagen nicht als Geschäftsbriefe an, sodass die entsprechenden Aufbewahrungsvorschriften der Abgabenordung nicht einschlägig sind.

Bei abgelehnten Bewerbern kann der Arbeitgeber die Bewerbungsunterlagen daher – im Hinblick auf etwaige Ansprüche wegen Diskriminierung nach dem AGG – bis zu sechs Monate vorhalten, um in der Lage zu sein, die Berechtigung solcher Ansprüche zu überprüfen; anschließend sind die Unterlagen zu löschen bzw. zu vernichten.

Wenn ein Bewerber eingestellt wird, werden seine Bewerbungsunterlagen Bestandteil der Personalakte und sind mindestens während seiner Betriebszugehörigkeit dort vorzuhalten.

Transparenzpflichten nach der DS-GVO

Frage des GDD Erfa-Kreises Würzburg:

Um den Transparenzpflichten nach der DS-GVO nachzukommen, wird eine elektronisch zur Verfügung gestellte Information (z.B. Datenschutzhinweis auf Homepage, Intranet) mit den aktuell geforderten gesetzlichen Inhalten an den geeigneten Stellen im Text, mit der Option "Mehr Lesen" versehen. Hierdurch soll verhindert werden, dass die Informationsflut den Betroffenen sogleich "erschlägt". Klickt er "Mehr Lesen" an, so würden die nach den neuen EU-Verordnungen geforderten Informationen sofort sichtbar .

Wäre dies ein gangbarer Weg?

Antwort des BayLDA:

Im Kurzpapier Nr. 10 der Datenschutzkonferenz, siehe z. B. die Veröffentlichung unter https://www.lda.bayern.de/media/dsk_kpnr_10_informationspflichten.pdf, sind nähere Erläuterungen der Datenschutzaufsichtsbehörden zu den Informationspflichten nach Art. 13 und 14 DS-GVO enthalten.

Zu der Anfrage wird speziell auf folgende Passagen in dem Kurzpapier hingewiesen: "Bei der Informationspflicht im Falle der Direkterhebung wird zwischen den Informationen unterschieden, die der betroffenen Person mitzuteilen sind (Art. 13 Abs. 1 DGS-GVO) und solchen, die zur Verfügung zu stellen sind, um eine faire und transparente Verarbeitung der personenbezogenen Daten zu gewährleisten (Art. 13 Abs. 2 DS-GVO). Bei der Direkterhebung müssen die Informationen zum Zeitpunkt der Erhebung der Daten mitgeteilt bzw. zur Verfügung gestellt werden.

Die leicht zugängliche Form bedeutet auch, dass die Informationen in der konkreten Situation verfügbar sein müssen. Sollen die Daten also von einer anwesenden Person erhoben werden, darf die Person in der Regel nicht auf Informationen im Internet verwiesen werden. "

Wenn es um Datenerhebungen von der betroffenen Person selbst über eine Internet- oder Intranet-Seite geht, z. B. per Anmeldeseite, Bestellseite oder Kontaktformular usw., müssen die Informationen nach Art. 13 Abs. 1 und 2 DS-GVO nicht unmittelbar auf diesen Seiten stehen, sondern können auch in einer eindeutigen und leicht zugänglichen Form verlinkt werden.

Die DSGVO in der Bundesverwaltung

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat einen neuen Leitfaden mit den Namen "Die DSGVO in der Bundesverwaltung" veröffentlicht. Der Leitfaden soll einen ersten praktischen Überblick über die umzusetzenden Vorgaben geben. Er richtet sich in erster Linie an diejenigen Organisationseinheiten aller öffentlichen Stellen des Bundes, die vor Ort für die Einhaltung des Datenschutzes Sorge tragen, und gibt darüber hinaus auch den Datenschutzbeauftragten aller öffentlichen Stellen des Bundes ein Werkzeug zur Erfüllung ihrer Aufgaben an die Hand.

Der Inhalt des Leitfadens dürfte aber auch für alle Verantwortlichen außerhalb der öffentlichen Stellen des Bundes lehr- und hilfreich sein. Ausführlich behandelte Themen sind bspw.:

- Anforderungen an und Anpassung von Verfahren
- Rechtsgrundlagen
- Umsetzung der Betroffenenrechte

Quelle: Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)

Datenverarbeitung in der Steuerberatung

Mit der Frage, ob die von Steuerberatern erbrachten Dienstleistungen eher als Auftragsverarbeitung zu betrachten sind oder als Inanspruchnahme fremder Fachleistungen bei einem eigenständig Verantwortlichen, für die bei der Verarbeitung (einschließlich Übermittlung) personenbezogener Daten eine Rechtsgrundlage gemäß Art. 6 DS-GVO gegeben sein muss, hatte sich die Datenschutzkonferenz bereits in ihrem Kurzpapier Nr. 13 "Auftragsverarbeitung, Art. 28 DS-GVO" befasst.
Darin heißt es:
"[…] Auftragsverarbeitung können regelmäßig z. B. folgende Dienstleistungen sein:
DV-technische Arbeiten für die Lohn- und Gehaltsabrechnung oder die Finanzbuchhaltung durch Rechenzentren, […]" und "Keine Auftragsverarbeitung, sondern die Inanspruchnahme fremder Fachleistungen bei einem eigenständig Verantwortlichen, für die bei der Verarbeitung (einschließlich Übermittlung) personenbezogener Daten eine Rechtsgrundlage gemäß Art. 6 DS-GVO gegeben sein muss, sind beispielsweise in der Regel die Einbeziehung eines Berufsgeheimnisträgers (Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer) [..]".
Aktuell äußert sich die LDI NRW konkret zu dieser Fragestellung und stellt fest, dass die vertraglichen Aufgabenfestlegungen zwischen dem Mandanten und dem Steuerberater entscheiden sind. Eine Datenverarbeitung im Auftrag gemäß Art. 28 Datenschutz-Grundverordnung (DS-GVO) sei in den Fällen zu bejahen, in denen einem Steuerberater eine Aufgabe ohne eigene Entscheidungskompetenzen übertragen werde. Dies sei etwa bei der reinen Lohn- und Gehaltsabrechnung der Fall oder bei sonstigen, rein technischen Dienstleistungen. Erforderlich sei dann ein Vertrag zur Auftragsverarbeitung.
Eine Datenverarbeitung in eigener Verantwortung sei hingegen bei weisungsunabhängigen Aufgaben oder Dienstleistungen gegeben – etwa die Erstellung des Jahresabschlusses oder die klassische Steuerberatung. Nach § 32 Abs. 2 Steuerberatungsgesetz (StBerG) in Verbindung mit den tätigkeitsbeschreibenden Normen im StBerG handeln Steuerberater eigenverantwortlich und damit aufgrund gesetzlicher Vorgaben weisungsfrei, so die LDI NRW. In diesem Fall seien sie keine Auftragnehmer im Sinne des Art. 28 DS-GVO.
Bei gemischten Tätigkeiten – eigenverantwortliche Steuerberatung sowie weisungsgebundene Dienstleistungen – sei zu differenzieren: Im Hinblick auf weisungsgebundene Dienstleistungen ist eine Auftragsverarbeitung gegeben, im Hinblick auf die Beauftragung mit Tätigkeiten aufgrund steuerberatungsrechtlicher Vorschriften eine Datenverarbeitung in eigener Verantwortung.
Übermittle zum Beispiel ein Arbeitgeber im Zusammenhang mit der Erstellung des Jahresabschlusses auch Daten zum Zwecke der Lohn- und Gehaltsabrechnung an den Steuerberater, so liege hinsichtlich dieser untergeordneten Tätigkeit keine Datenverarbeitung in eigener Verantwortung vor.

Quelle: LDI NRW

ULD-Reihe: Videoüberwachung nach DS-GVO

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) setzt seine Praxis-Reihe: "Datenschutzbestimmungen praktisch umsetzen" mit einem neuen Leitfaden fort. Das fünfte Werk aus der Reihe beschäftigt sich mit dem Thema Videoüberwachung.
Die Broschüre gibt Auskunft über die wichtigsten Fragen zum Datenschutz bei Videoüberwachung durch private Stellen aus der Sicht von Verantwortlichen und betroffenen Personen. Es geht also nicht um die Videoüberwachung durch den Staat, hier gelten nochmals besondere Regeln. Nicht enthalten sind Fragen der Veröffentlichung von Video- oder Bildmaterial. Hierzu gibt es die Broschüre Fotos und Webcams der Praxisreihe.

Die Broschüre behandelt folgende Einzelfragen:

1. Wie kann eine Videoüberwachungsanlage rechtmäßig betrieben werden?
2. Wie muss über die Videoüberwachung informiert werden?
3. Gelten diese Voraussetzungen auch im rein privaten oder familiären Bereich?
4. Wie muss das System der Videoüberwachung aufgebaut sein?
5. Wie lange dürfen die Aufzeichnungen gespeichert werden?
6. Dürfen auch weiträumige Areale überwacht werden?
7. Gelten die Anforderungen auch für Attrappen?
8. Konkrete Fallbeispiele.
9. Was passiert, wenn die notwendigen Anforderungen nicht einhalten werden?
10. An wen kann ich mich als Betroffener wenden?
11. Welche Rechte habe ich als Betroffene(r)?

Quelle: ULD

Gesonderte Entgeltpflicht für Kontrolle m Rahmen der Auftragsverarbeitung

Im Rahmen seiner sog. "Aktuellen Kurzinformationen" (AKI) weist der BayLfD auf einen Umstand hin, der viele der Parteien einer Auftragsverarbeitung betreffen dürfte.
Es kommt nicht selten vor, dass Vereinbarungen zur Auftragsverarbeitung vorsehen, dass es dem Auftraggeber nur gegen Zahlung eines besonderen Entgelts möglich sein soll, eine Vor-Ort-Kontrolle bei dem Auftragsverarbeiter durchzuführen.
So enthält bspw. auch das Muster der GDD unter Ziffer 7 (4) folgende Musterklausel:
"Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltende machen".
Der BayLfD weisst in seiner aktuellen AKI darauf hin, dass die Wahrnehmung der Kontrollrechte aus datenschutzrechtlicher Sicht nicht von einem besonderen Entgelt abhängig gemacht werden darf. Dies gelte gerade auch für Vor-Ort-Kontrollen beim Auftragsverarbeiter.
Ein besonderes Entgelt würde einer Ausübung der Kontrollrechte entgegenwirken.
Die Vereinbarung eines Entgelts, einer Aufwandsentschädigung oder eines sonstiges Kostenbeitrags, auch die Vereinbarung, hierzu im Bedarfsfall nachträglich eines Regelung zu treffen, führe dazu, dass eine Inspektion beim Auftragsverarbeiter als etwas "Außergewöhnliches" wahrgenommen werde, das dem Auftraggeber "eigentlich" zustehe und gerade deshalb außerhalb der wechselseitigen Austauschbeziehung zu vergüten sei.
Unbenommen bleibe es dem Auftragsverarbeiter aber, die ihm durch Vor-Ort-Kontrollen seines Auftraggebers entstehenden Kosten von vornherein pauschal in das Angebot der vertraglichen Leistung einzupreisen.

Quelle: Der Bayrische Landesbeauftragte für den Datenschutz

EU und Japan erkennen beiderseits angemessenes Datenschutzniveau an

Die EU und Japan haben am 17. Juli 2018 ihre Gespräche über ein beiderseits angemessenes Datenschutzniveau erfolgreich abgeschlossen. Sie haben sich darauf verständigt, die Datenschutzsysteme der jeweils anderen Seite als "gleichwertig" anzuerkennen, sodass Daten zwischen der EU und Japan sicher fließen können. Jede Seite wird nun ihre jeweiligen internen Verfahren für die Annahme ihrer Angemessenheitsfeststellung einleiten. Im Falle der EU gehören dazu die Einholung einer Stellungnahme des Europäischen Datenschutzausschusses sowie die Zustimmung eines Ausschusses, der sich aus Vertretern der EU-Mitgliedstaaten zusammensetzt. Sobald dieses Verfahren abgeschlossen ist, wird die Kommission den Angemessenheitsbeschluss in Bezug auf Japan annehmen.
Mit dieser Vereinbarung bekräftigen die EU und Japan, dass die Förderung hoher Datenschutzstandards und die Erleichterung des internationalen Handels im digitalen Zeitalter Hand in Hand gehen. Im Rahmen der Datenschutz-Grundverordnung ist ein Angemessenheitsbeschluss der einfachste Weg, um sichere und stabile Datenströme zu gewährleisten.
Die getroffene Vereinbarung sieht die gegenseitige Anerkennung eines gleichwertigen Datenschutzniveaus durch die EU und Japan vor. Nach Annahme werden mit dieser Vereinbarung personenbezogene Daten geschützt, die zu gewerblichen Zwecken übertragen werden, aber auch solche, die zu Strafverfolgungszwecken zwischen den Behörden der EU und Japans ausgetauscht werden, sodass sichergestellt wird, dass bei all diesen Übermittlungen ein hohes Datenschutzniveau zur Anwendung kommt.

Quelle: EU-Kommission

Abgrenzung der Auftragsverarbeitung nach der DS-GVO

Unter der neu geschaffenen Rubrik "Fragen & Antworten" nimmt das BayLDA ausführlich Stellung zu verschiedenen Fragestellungen des Datenschutzes. Um die gegebenen Antworten einzuordnen, wird jede Frage/Antwort zusätzlich mit nützlichen Stichworten und Normen versehen.
Das Bayrische Landesamt für Datenschutzaufsicht hat seine Reihe "FAQ zur DS-GVO" um die Beantwortung einer weiteren Praxisfrage ergänzt.
Die aktuellste Frage der FAQ-Sammlung beschäftigt sich mit den Art. 4 Nr. 8, 28 DS-GVO. Darin versucht das BayLDA anhand konkreter Fallbeispiele zu zeigen, bei welcher Art von Datenverarbeitung eine Auftragsverarbeitung anzunehmen ist und wann nicht.
Auftragsverarbeitung im datenschutzrechtlichen Sinne liege nur in Fällen vor, in denen eine Stelle von einer anderen Stelle im Schwerpunkt mit der Verarbeitung personenbezogener Daten beauftragt werde, so das BayLDA.
Die Beauftragung mit fachlichen Dienstleistungen anderer Art, d. h., mit Dienstleistungen, bei denen nicht die Datenverarbeitung im Vordergrund stehe bzw. bei denen die Datenverarbeitung nicht zumindest einen wichtigen (Kern-)Bestandteil ausmache, stelle keine Auftragsverarbeitung im datenschutzrechtlichen Sinne dar.
Als Auftragsverarbeitung im Sinne von Art. 4 Nr. 8 DS-GVO werden (u.a.) bspw. folgende Verarbeitungen gesehen:

- DV-technische Arbeiten für die Lohn- und Gehaltsabrechnung oder die Finanzbuchhaltung durch Rechenzentren,
- Outsourcing personenbezogener Datenverarbeitung im Rahmen von Cloud-Computing, ohne dass ein inhaltlicher Datenzugriff des Cloud-Betreibers erforderlich ist,

Keine Auftragsverarbeitung im Sinne von Art. 4 Nr. 8 DS-GVO (sondern eigene Verantwortlichkeit) sei (u.a.) z. B. regelmäßig:

a) Inanspruchnahme fremder Fachleistungen bei einem eigenständig Verantwortlichen
   - Tätigkeiten der Berufsgeheimnisträger (Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer),
   - Inkassobüros mit Forderungsübertragung,
   - Bankinstitute für den Geldtransfer

b) im Kern keine beauftragte Verarbeitung personenbezogener Daten, sondern der Auftragsziele auf eine andere Tätigkeit:
   - vom Vermieter beauftragte Handwerker, die dazu die nötigen Mieterdaten erhalten,
   - Sachverständige zur Begutachtung eines Kfz-Schadens,
   - Personenbeförderung, Krankentransportleistungen

Das BayLDA weist jedoch darauf hin, dass, je nach Sachverhalt, vom Verantwortlichen ggfls. Zweckbindung und Vertraulichkeit zu den dabei berührten personenbezogenen Daten festzulegen sein kann.

Datenschutzstandards bei grenzüberschreitender Strafverfolgung

Die Internationale Arbeitsgruppe für Datenschutz in der Telekommunikation (sog. Berlin Group), die von der Berliner Beauftragten für Datenschutz und Informationsfreiheit, Frau Maja Smoltczyk, geleitet wird, hat auf ihrer 63. Sitzung am 9. und 10. April 2018 in Budapest (Ungarn) das Arbeitspapier Standards für den Datenschutz und den Schutz der Privatsphäre bei grenzüberschreitenden Datenanforderungen zu Strafverfolgungszwecken verabschiedet.

Da Daten weltweit immer mehr ausgetauscht und gespeichert werden, erbitten Strafverfolgungsbehörden bei Ermittlungen immer häufiger den Zugang zu personenbezogenen Daten, die sich außerhalb ihrer Landesgrenzen befinden. Angesichts dieser Entwicklungen arbeiten Regierungen und internationale Organisationen verstärkt an Maßnahmen für einen erleichterten Zugang zu Cloud-Daten. Die grenzüberschreitenden Auskunftsersuchen werfen jedoch komplizierte datenschutzrechtliche Fragen auf.

Traditionelle Regelungen zur internationalen Koordinierung durch die Strafverfolgungsbehörden gelten mit Blick auf die zunehmende Häufigkeit und Komplexität grenzüberschreitender Datenanfragen als zu schwerfällig. Alternative Mechanismen, wie etwa freiwillige Vereinbarungen zwischen Anbietern und ausländischen Behörden, können unterschiedlichen und intransparenten Standards unterworfen sein. Fehlt es an Rechtskraft, bieten sie wenig Sicherheit für den Schutz der Rechte der betroffenen Personen.

Die Internationale Arbeitsgruppe für Datenschutz in der Telekommunikation skizziert in ihrem kürzlich veröffentlichten Arbeitspapier die aktuellen Entwicklungen im Bereich grenzüberschreitender Datenabfragen für die Strafverfolgung. Sie fordert die beteiligten Akteure dazu auf, bei der Förderung einer schnellen Bearbeitung legitimer grenzüberschreitender Datenanfragen, die Interessen des Datenschutzes und der Privatsphäre stets zu wahren und gibt Empfehlungen, wie dies gewährleistet werden kann.

Das Arbeitspapier kann unter http://www.berlin-privacy-group.org abgerufen werden.

Quelle: BlnBDI

Neue Datenethikkommission tagt im September

Der Einsatz von Algorithmen, künstlicher Intelligenz und digitalen Innovationen birgt große Potenziale. Gleichzeitig stellen sich zahlreiche ethische und rechtliche Fragen. Die Datenethikkommission der Bundesregierung soll hierauf Antworten geben.
Neue datenbasierte Technologien verbessern den Alltag des Einzelnen, sie stiften Nutzen für Wirtschaft, Wissenschaft und die Gesellschaft als Ganzes. Ihr Einsatz wirft aber auch Fragen auf: Was verändert sich durch den Einsatz im Leben der Bürgerinnen und Bürger, in der Wirtschaft und in der Gesellschaft als Ganzes? Welche Rolle wollen wir den neuen Technologien in der Zukunft zukommen lassen?
Die Antworten auf solche Fragen müssen viele Blickwinkel berücksichtigen, z.B. aus technischer, ethischer, rechtlicher oder gesellschaftswissenschaftlicher Sicht. Um all diese Sichtweisen zu Wort kommen zu lassen, und in einer gemeinsamen Diskussion über unsere Zukunft zusammenzuführen, haben die Regierungsparteien im Koalitionsvertrag die Einsetzung einer Datenethikkommission der Bundesregierung vereinbart:
"Wir werden zeitnah eine Datenethikkommission einsetzen, die Regierung und Parlament innerhalb eines Jahres einen Entwicklungsrahmen für Datenpolitik, den Umgang mit Algorithmen, künstlicher Intelligenz und digitalen Innovationen vorschlägt. Die Klärung datenethischer Fragen kann Geschwindigkeit in die digitale Entwicklung bringen und auch einen Weg definieren, der gesellschaftliche Konflikte im Bereich der Datenpolitik auflöst."
Die Datenethikkommission soll auf der Basis wissenschaftlicher und technischer Expertise ethische Leitlinien für den Schutz des Einzelnen, die Wahrung des gesellschaftlichen Zusammenlebens und die Sicherung des Wohlstands im Informationszeitalter entwickeln. Sie wird der Bundesregierung unter Federführung des Bundesministeriums des Innern, für Bau und Heimat und des Bundesministeriums der Justiz und für Verbraucherschutz bis Sommer 2019 Handlungsempfehlungen geben und Regulierungsmöglichkeiten vorschlagen.
Die Bundesregierung hat am 18. Juli 2018 die folgenden 16 Personen in die Datenethikkommission berufen:

- Johanna Haberer
- Marit Hansen
- Dirk Heckmann
- Dieter Kempf
- Mario Martini
- Klaus Müller
- Paul Nemitz
- Sabine Sachweh
- Christin Schäfer
- Rolf Schwartmann
- Judith Simon
- Andrea Voßhoff
- Wolfgang Wahlster
- Christiane Wendehorst (Co-Sprecherin)
- Thomas Wischmeyer
- Christiane Woopen (Co-Sprecherin)

Am 5. September 2018 werden Herr Bundesminister Seehofer und Frau Bundesministerin Dr. Barley die Mitglieder der Datenethikkommission zu ihrer ersten Sitzung im Bundesministerium des Innern für Bau und Heimat in Berlin begrüßen.

Quelle: Bundesministerium des Innern, für Bau und Heimat

Eigene Webseite der Datenschutzkonferenz geht online

Die Datenschutzkonferenz (DSK) besteht aus den unabhängigen Datenschutzbehörden des Bundes und der Länder. Sie hat die Aufgabe, die Datenschutzgrundrechte zu wahren und zu schützen, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen und gemeinsam für seine Fortentwicklung einzutreten. Dies geschieht namentlich durch Entschließungen, Beschlüsse, Orientierungshilfen, Standardisierungen, Stellungnahmen, Pressemitteilungen und Festlegungen.
Die Datenschutzkonferenz geht mit einer eigenen Homepage online. Auf der zentralen Informationsplattform sind aktuelle Entschließungen, Orientierungshilfen und Kurzpapiere der Datenschutzkonferenz abrufbar. Hier finden sich auch Links zu den Aufsichtsbehörden und den Datenschutzgesetzen des Bundes und der Länder. Zudem ist ein RSS-Feed zum Abonnieren neuer Inhalte eingebunden. Mit Anwendung der Datenschutz-Grundverordnung wird ihre Auslegung auch durch die Datenschutzaufsichtsbehörden wichtiger. Mit einer eigenen Homepage der Datenschutzkonferenz optimiert diese ihr Informationsangebot. Die Entwicklung der Webseite steht unter der Verantwortung des Bayerischen Landesamts für Datenschutzaufsicht.

Die Homepage der DSK ist unter https://www.datenschutzkonferenz-online.de/ zu erreichen.

FAQ: Datenschutz im Verein

ie DS-GVO entfaltet ihre Wirkung nicht nur für gewerbliche Unternehmen, sondern auch für alle Vereine. Auch diese haben die Verpflichtung, staatliche Regeln zu befolgen, auch jene zum Schutz der persönlichen Daten von Mitgliedern, Mitarbeitern und Vereinspartnern. Auch Vereinsvorstände befassen sich daher seit geraumer Zeit mit den Fragen des Datenschutzes rund um die DS-GVO.
Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Dr. Stefan Brink, hatte dies zum Anlass genommen, eine Orientierungshilfe zu dieser Thematik vorzustellen. Der Landesbeauftragte hierzu: "Für Vereine ist jetzt die Zeit gekommen, die neuen Datenschutz-Anforderungen in Angriff zu nehmen, damit der Übergang auf das neue Datenschutzrecht glatt über die Bühne gehen kann. Mit unserer Orientierungshilfe möchten wir den Vereinen zur Seite stehen und sie bei dieser Aufgabe unterstützen."
Auch das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) beantwortet die 10 am häufigsten gestellten Fragen zur Umsetzung der DS-GVO auf seiner Seite. Dabei werden geht es um folgende Fragen, die im Vereinsumfeld oft auftauchen:

- Muss mein Verein einen Datenschutzbeauftragten benennen?
- Darf mein Verein noch Mannschaftsfotos auf der eigenen Vereinshomepage veröffentlichen?
- Brauche ich als Verein ein "Verzeichnis der Verarbeitungstätigkeiten"?
- Dürfen unsere Spieler untereinander mit einem Messenger-Dienst kommunizieren?
- Benötige ich auf meiner Vereinswebseite HTTPS?
- Darf mein Verein Bilder von Spielszenen eines Fußballspiels ohne weitere Voraussetzungen veröffentlichen?
- Darf mein Verein Videos über Auftritte bei Vereinsveranstaltungen auf YouTube veröffentlichen?
- Darf mein Verein noch Vereinsinformationen per E-Mail an die Mitglieder versenden?
- Ist es erforderlich, von allen (aktiven und passiven) Vereinsmitgliedern eine schriftliche Einwilligungserklärung zur Datenverarbeitung einzuholen?
- Benötigt mein Verein von allen Vereinsmitgliedern nachträglich Einverständniserklärungen für veröffentlichte Bilder auf der Homepage bzw. in der Vereinszeitung?

Quelle: Bayerisches Landesamt für Datenschutzaufsicht

Bundesregierung möchte Schutz von Whistleblowern stärken

Die Bundesregierung hat am 18.07.2018 den von Bundesministerin der Justiz und für Verbraucherschutz, Dr. Katarina Barley, vorgelegten Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung beschlossen. Mit der Richtlinie wird ein europaweit einheitlicher Mindestschutz für Geschäftsgeheimnisse gewährleistet. Zugleich werden erstmals ausdrückliche Regelungen für den Schutz von Whistleblowern geschaffen.
Kernstück des Gesetzentwurfs ist das neue Gesetz zum Schutz von Geschäftsgeheimnissen. Danach können Unternehmen bei einer unerlaubten Erlangung, Nutzung oder Offenbarung von Geschäftsgeheimnissen zivilrechtliche Ansprüche wie Unterlassung und Schadensersatz geltend machen. Der bereits bestehende Schutz im deutschen Recht wird damit verbessert und die Rechtssicherheit für Unternehmen erhöht.
Auch der Schutz von Geschäftsgeheimnissen vor einer Offenlegung im Rahmen eines gerichtlichen Verfahrens wird verbessert. So können streitgegenständliche Informationen bei Einreichung einer Klage als geheimhaltungsbedürftig eingestuft werden und dadurch der Personenkreis begrenzt werden, der Zugang zu Dokumenten und Verhandlungen hat, in denen Geschäftsgeheimnisse eröffnet werden.
Das Gesetz zum Schutz von Geschäftsgeheimnissen trägt zugleich dem Schutz von Whistleblowern und Journalisten Rechnung. Zu diesem Zweck enthält es Regelungen für Sachverhalte, in denen der Erwerb, die Nutzung oder die Offenlegung von Geschäftsgeheimnissen nicht rechtswidrig ist. Das gilt zum Beispiel für Fälle, in denen die Handlung der Ausübung der Meinungs- und Informationsfreiheit oder der Aufdeckung von Fehlverhalten und rechtswidrigen Handlungen dient.

Quelle: Bundesministerium der Justiz und für Verbraucherschutz

GDD-Praxishilfe: ePrivacy I

Seit dem 25. Mai 2018 ist die Datenschutz-Grundverordnung (DS-GVO) anwendungspflichtig. Auf Grund der Wahl einer Verordnung als unionsrechtlicher Rechtsakt gilt diese in der gesamten Europäischen Union (EU) unmittelbar und genießt einen Vorrang vor dem nationalen Recht. Mit diesem Tag begann aber auch die zeitliche Lücke zwischen DS-GVO und der noch ausstehenden ePrivacy-VO, die nach ursprünglicher Planung zum gleichen Tag hin anwendbar sein sollte.
Das bereichsspezifische Datenschutzrecht für elektrische Kommunikation ist bislang durch die ePrivacy-Richtlinie geregelt, die in Deutschland im TKG, TMG und UWG umgesetzt wurde. Um das Verhältnis zwischen der DS-GVO und der ePrivacy-Richtlinie klarzustellen, sollte die Richtlinie durch die ePrivacy-VO ersetzt werden. Keiner weiß momentan, wie die ePrivacy-VO am Ende genau aussehen wird. Sicher ist nur: Trotz Änderung des übergeordneten Datenschutzrechts durch die DS-GVO seit Mai diesen Jahres bleiben TKG und TMG unberührt.
Die neueste Praxishilfe der GDD "GDD-Praxishilfe: ePrivacy I- Aktueller Stand & Veränderungen durch die DS-GVO" stellt die aktuelle, rechtliche Lage vor, wirft einen Blick auf die mögliche zukünftige Lage (Regelungsinhalte der ePrivacy-VO) und arbeitet das allgemeine Verhältnis zwischen DSGVO und ePrivacy-RL in der Zwischenphase heraus.

Die neue Praxishilfe der GDD ist wie folgt abrufbar:
https://www.gdd.de/downloads/praxishilfen/001_ePrivacy_01.pdf

BGH urteilt zum digitalen Nachlass

57 Prozent der Deutschen nutzen lediglich ihr Gedächtnis, um sich ihre Online-Passwörter zu merken. Bei Flickr (und anderen Social-Media-Anbietern) können Freunde und Familie nicht auf die Fotos von Verstorben zugreifen.
Hinterbliebene stehen vor vielen Herausforderungen, wenn sie an Vertragsinformationen gelangen müssen und Online-Konten von Verstorbenen verwalten sollen. Ohne Passwörter und Zugangsdaten haben Erben oft keinen Zugriff auf die Online-Konten. Sie können sich nicht um laufende Geschäfte wie Internetauktionen, Abos oder Bestellungen kümmern oder Verträge kündigen. Im schlimmsten Fall entstehen hohe laufende Kosten und finanzielle Schäden. Nur wenige Unternehmen stellen bislang Regeln auf, unter welchen Bedingungen ein Account aufgelöst werden kann und wer darüber entscheiden darf. Manche Regelungen sind zudem rechtlich fragwürdig. Neben der rechtlichen Seite geht es aber auch um einen selbstbestimmten Umgang mit dem eigenen Nachlass, etwa um den Umgang mit Profilen in sozialen Netzwerken. Nun hat sich auch der BGH mit einer konkreten Fragestellung aus dieser Thematik beschäftigen müssen.
Der III. Zivilsenat des Bundesgerichtshofs hat am 12.07.2018 entschieden, dass der Vertrag über ein Benutzerkonto bei einem sozialen Netzwerk grundsätzlich im Wege der Gesamtrechtsnachfolge auf die Erben des ursprünglichen Kontoberechtigten übergeht und diese einen Anspruch gegen den Netzwerkbetreiber auf Zugang zu dem Konto einschließlich der darin vorgehaltenen Kommunikationsinhalte haben.
Die Klägerin ist die Mutter der im Alter von 15 Jahren verstorbenen L. W. und neben dem Vater Mitglied der Erbengemeinschaft nach ihrer Tochter. Die Beklagte betreibt ein soziales Netzwerk, über dessen Infrastruktur die Nutzer miteinander über das Internet kommunizieren und Inhalte austauschen können.
2011 registrierte sich die Tochter der Klägerin im Alter von 14 Jahren im Einverständnis ihrer Eltern bei dem sozialen Netzwerk der Beklagten und unterhielt dort ein Benutzerkonto. 2012 verstarb das Mädchen unter bisher ungeklärten Umständen infolge eines U-Bahnunglücks.
Die Klägerin versuchte hiernach, sich in das Benutzerkonto ihrer Tochter einzuloggen. Dies war ihr jedoch nicht möglich, weil die Beklagte es inzwischen in den sogenannten Gedenkzustand versetzt hatte, womit ein Zugang auch mit den Nutzerdaten nicht mehr möglich ist. Die Inhalte des Kontos bleiben jedoch weiter bestehen.
Die Klägerin beansprucht mit ihrer Klage von der Beklagten, den Erben Zugang zu dem vollständigen Benutzerkonto zu gewähren, insbesondere zu den darin vorgehaltenen Kommunikationsinhalten. Sie macht geltend, die Erbengemeinschaft benötige den Zugang zu dem Benutzerkonto, um Aufschluss darüber zu erhalten, ob ihre Tochter kurz vor ihrem Tod Suizidabsichten gehegt habe, und um Schadensersatzansprüche des U-Bahn-Fahrers abzuwehren.
Das Landgericht hat der Klage stattgegeben. Auf die Berufung der Beklagten hat das Kammergericht das erstinstanzliche Urteil abgeändert und die Klage abgewiesen. Hiergegen richtet sich die vom Berufungsgericht zugelassene Revision der Klägerin.
Das Gericht hat insbesondere festgestellt, dass schließlich der Anspruch der Klägerin auch nicht mit dem Datenschutzrecht kollidiert. Der Senat hat hierzu die seit 25. Mai 2018 geltende Datenschutz-Grundverordnung (DS-GVO) angewendet. Diese stehe dem Zugang der Erben nicht entgegen. Datenschutzrechtliche Belange der Erblasserin seien nicht betroffen, da die Verordnung nur lebende Personen schütze. Die der Übermittlung und Bereitstellung von Nachrichten und sonstigen Inhalten immanente Verarbeitung der personenbezogenen Daten der Kommunikationspartner der Erblasserin sei sowohl nach Art. 6 Abs. 1 Buchst. b Var. 1 DS-GVO als auch nach Art. 6 Abs. 1 Buchst. f DS-GVO zulässig. Sie sei sowohl zur Erfüllung der vertraglichen Verpflichtungen gegenüber den Kommunikationspartnern der Erblasserin erforderlich (Art. 6 Abs. 1 Buchst. b Var. 1 DS-GVO) als auch auf Grund berechtigter überwiegender Interessen der Erben (Art. 6 Abs. 1 Buchst. f DS-GVO).

Quelle: Bundesgerichtshof