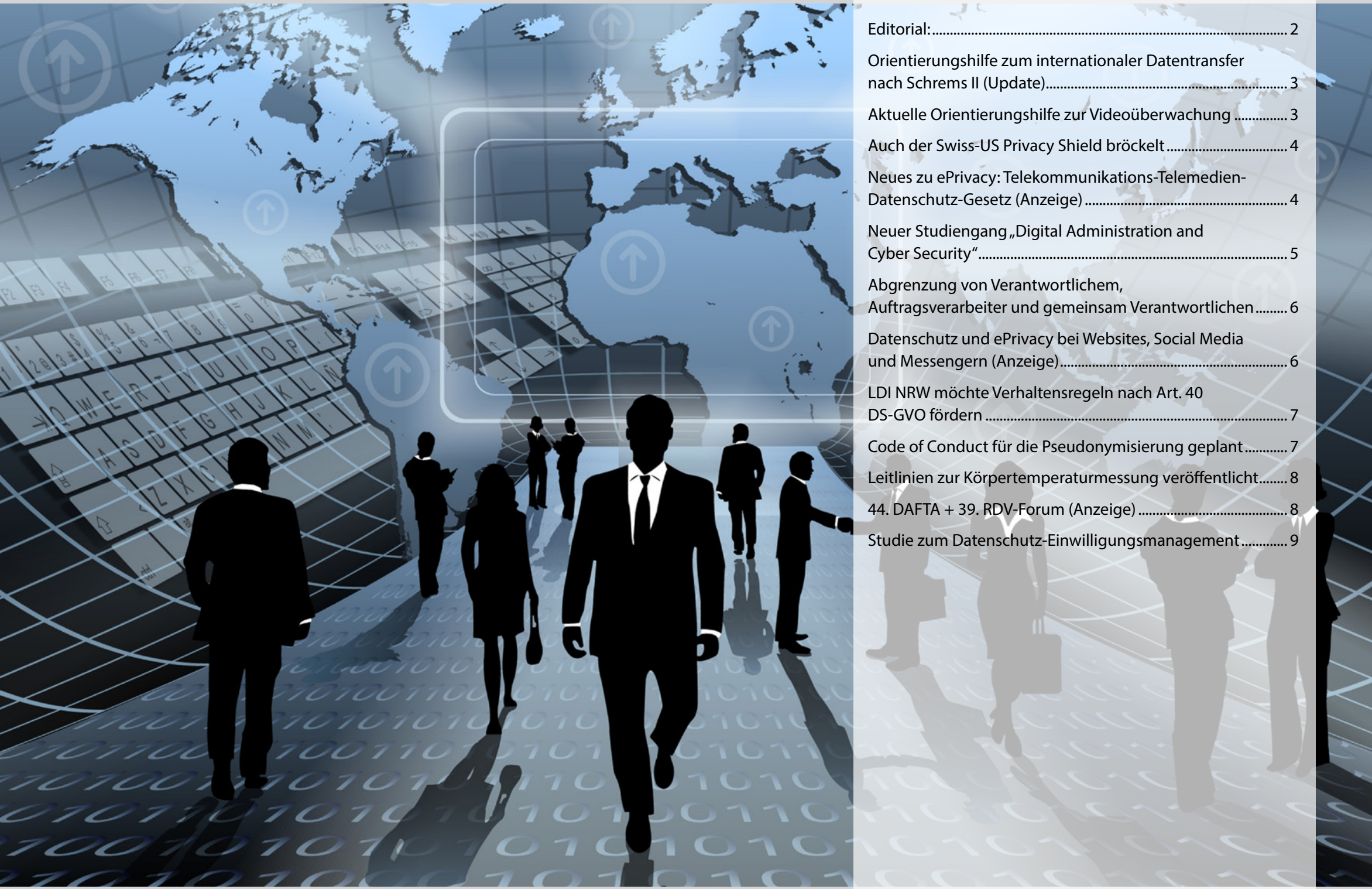
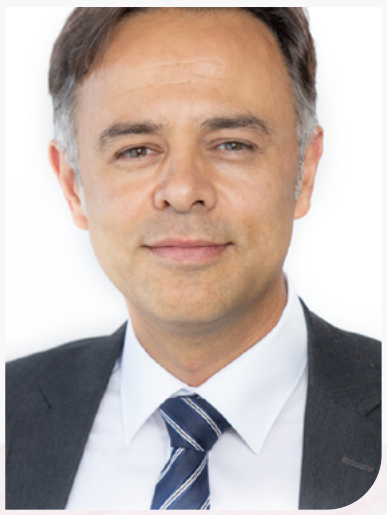
Datenschutz newsbox

Ausgabe 09 2020



DATAKONTEXT



Editorial:

Was den Idealtypus eines Verbrauchers für einige Unternehmen und die Schufa angeht, scheint zu gelten: „Er/Sie soll bitte viel konsumieren, aber bloß nichts hinterfragen oder gar Preis und Leistung verschiedener Anbieter vergleichen“. Wenn doch, ist er/sie schon mal sehr verdächtig und ggf. unerwünscht. Anders lässt sich nicht erklären, wie sog. Wechselkunden, bei einigen Energieversorgern auch „Bonushopper“ genannt, behandelt werden (sollen).
Ist ein Kunde/Betroffener aber zu unauffällig/passiv und daher ein „unbeschriebenes Blatt“ ist das zumindest einigen Wirtschaftsauskunfteien auch wieder nicht recht. Auf diesen Fall hatte der LfDI BW vor einiger Zeit hingewiesen. Ermahnt wurde dort die Praxis einer Wirtschaftsauskunftei. Der Datenschutzbeauftragte stellte auf Grund von zahlreichen Beschwerden fest, dass Bonitätsbeurteilungen nicht immer anhand konkret vorliegender Daten des jeweiligen Unternehmens vorgenommen wurden, sondern gerade nicht vorliegende Informationen dazu führten, dass der empfohlene Kreditrahmen niedrig eingestuft wurde. Wie man es macht, ist es also falsch.

Aber auch bei Aufsichtsbehörden gibt es widersprüchliches Verhalten. So war jüngst zu lesen, dass der Hessische Beauftragte für Datenschutz und Informationsfreiheit (HBDI) „im Interesse einer flexiblen Bekämpfung der Corona-Pandemie übergangsweise den Einsatz von Videokonferenzsystemen in Schulen weitgehend für alle zur Verfügung stehenden Anwendungen auf der Grundlage von Art. 6 Abs. 1 Buchst. d) und e) der Datenschutz-Grundverordnung (DS-GVO) duldet, auch wenn deren Datenschutzkonformität noch nicht abschließend geklärt ist“. Nicht ganz so weit von Hessen entfernt, hört sich das gar nicht mehr so pragmatisch an, wenn es dort lautet: „Schulen sollten stattdessen auf europäische Anbieter zurückgreifen und solche bevorzugen, bei denen keine Verarbeitung der Daten von Nutzerinnen und Nutzer stattfindet“. Der Umstand, dass Wirtschaftsprüfer von PricewaterhouseCoopers (PWC) und eine Aufsichtsbehörde bzgl. der Datenschutzkonformität von Office 365 und der Qualität der dazu existierenden Datenschutz-Folgenabschätzung nicht derselben Meinung sind, verwundert da schon weniger, 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

Orientierungshilfe zum internationaler Datentransfer nach Schrems II (Update)

Der EuGH hat das EU-Privacy Shield mit seinem Urteil vom 16.07.2020 (Az: C-311/18) für ungültig erklärt und an die Pflichten für Datenexporteure und Datenimporteure bei Anwendung der EU-Standardvertragsklauseln, insbesondere hinsichtlich einer rechtskonformen Datenübermittlung, erinnert. Datenexportierende verantwortliche Stellen mit Sitz in der Europäischen Union oder in Ländern des Europäischen Wirtschaftsraums stehen seitdem vor der Herausforderung, wie personenbezogene Daten weiterhin rechtskonform in Drittländer übermittelt werden können.

Nach dem bereits Akteure wie der Europäische Datenschutzausschuss oder Verbände wie die GDD versucht haben mit FAQs oder Handlungsempfehlungen ein wenig mehr Rechtssicherheit für die Verantwortlichen zu schaffen, verblieben doch immer noch mehr Fragen als Antworten. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg brachte mit einem neuen Vorstoß noch mehr Licht ins Dunkel in dem er weitere Hinweise zum Fall Schrems II gab und zugleich sein weiteres Vorgehen in Form einer Orientierungshilfe zum Urteil des Europäischen Gerichtshofs (EuGH) vom 16. Juli 2020, Rechtssache C-311/18 („Schrems II“) festlegte.
Die in der Orientierungshilfe beantworteten Fragen und die Antworten darauf wurden nun von der Aufsichtsbehörde aktualisiert. Die Orientierungshilfe beschäftigt sich mit folgenden Fragestellungen:
Worum geht`s? / Kernaussagen des Urteils
Wen betrifft die Entscheidung?
Was bedeutet die Entscheidung konkret? / Was ist zu tun?
Wo und wie anfangen? / Checkliste

Quelle: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg

Aktuelle Orientierungshilfe zur Videoüberwachung

Unter der Redaktion des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg hat die DSK eine neue Orientierungshilfe mit dem Titel „Videoüberwachung durch nicht-öffentliche Stellen“ veröffentlicht.

Die umfangreich aktualisierte Orientierungshilfe trägt dem Umstand Rechnung, dass Videoüberwachungsanlagen in großer Zahl eingesetzt werden und damit, sich die Verletzung der Rechte von Betroffenen in den vergangenen Jahren deutlich erhöht hat. Als eine der Gründe sieht die Orientierungshilfe die geringen Anschaffungskosten und die verbesserte Qualität der Technik an. Moderne Kameras zeigten Bilder in höchster Auflösung. In Echtzeit könnten diese in der ganzen Welt eingesehen und fast unbegrenzt gespeichert werden. Mehr als ein Smartphone oder Tablet brauche es oft nicht.

Hinzu komme jedoch, dass Kameras nicht nur zur Sicherheit eingesetzt würden, sondern Daten von Personen erfassen und verarbeiten, um bspw. personalisierte Werbung anzuzeigen oder Produkte zielgruppengenau anzubieten. Softwaregesteuerte Videotechnik vermesse in der Öffentlichkeit Gesichtszüge und Gefühlsregungen von Personen oder verfolgt das Bewegungs- oder Einkaufsverhalten von Kunden. Der Betroffene habe kaum Einfluss auf eine solche Erfassung und erfährt selten, was mit den Aufnahmen geschehe.

Besonders für die Praktiker dürften die Kapitel 3. „Maßnahmen vor der Durchführung“, der auch einen Abschnitt zur Durchführung einer „Datenschutz-Folgenabschätzung“ enthält sowie die Ausführungen zur „Überwachung von Beschäftigten“ in Kapitel 5.1 von gesteigertem Interesse sein.

Auch der Swiss-US Privacy Shield bröckelt

Anfang 2017 ersetzte der neue «Swiss-US Privacy Shield» das Safe Harbor-Abkommen (Safe Harbor Framework) zwischen der Schweiz und den USA. Der Europäische Gerichtshof (EuGH) hatte diesen «sicheren Hafen» im Verhältnis zwischen der EU und den USA im Oktober 2015 für ungültig erklärt In der Folge vertrat der Eidgenössische Datenschutz- und Öffentlichtskeitsbeauftragte (EDÖB) die Meinung, auch das inhaltlich weitgehend identische amerikanisch-schweizerische Safe Harbor-Abkommen genüge nicht mehr.
Aber auch schon damals lastete auf dem Swiss-US Privacy Shield derselbe Makel wie auf der Variante der EU. Schon damals bemängelten Kritiker dieselben Punkte wie beim EU-US Privacy Shield, so dass jedem klar war, dass wenn der EuGH früher oder später voraussichtlich über den Privacy Shield zwischen der EU und den USA urteilen muss, dies wiederum Auswirkungen auf die Schweiz haben würde – wie schon zuvor beim EuGH-Urteil gegen das Safe Harbor Framework.

Daher kam es nun, wie es kommen musste:
Vor dem Hintergrund seiner jährlichen Überprüfungen des Swiss-US Privacy Shields Regimes sowie der jüngsten Rechtsprechung des Europäischen Gerichtshofs (EuGH) zum Datenschutz evaluierte der Eidgenössische Datenschutz- und Öffentlichkeitbeauftragte (EDÖB) die Datenschutzkonformität des Privacy Shield Regimes neu.
Nach vertiefter Analyse kam der EDÖB in seiner Stellungnahme vom 8.9.2020 zum Schluss, dass das Privacy Shield Regime trotz der Gewährung von besonderen Schutzrechten für Betroffene in der Schweiz kein adäquates Schutzniveau für Datenbekanntgaben von der Schweiz an die USA gemäß Bundesgesetz über den Datenschutz (DSG) bietet. Aufgrund dieser auf das schweizerische Recht gestützten Einschätzung hat der EDÖB in der Staatenliste des EDÖB den Verweis auf einen «angemessenen Datenschutz unter bestimmten Bedingungen» für die USA gestrichen. Da die Einschätzung des EDÖB keinen Einfluss auf das Weiterbestehen des Regimes des Privacy Shield hat und sich betroffene Personen darauf berufen können, solange dieses seitens der USA nicht widerrufen wird, werden die Bemerkungen zum Privacy Shield in der Länderliste in angepasster Form beibehalten.

Quelle: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

Neuer Studiengang „Digital Administration and Cyber Security“

Im kommenden Wintersemester wird ein weiteres Kapitel in der „Digitalen Agenda“ der Bundesregierung aufgeschlagen. Dann startet an der Hochschule des Bundes für öffentliche Verwaltung (HS Bund) in Brühl der Studiengang „Digital Administration and Cyber Security“ – kurz DACS. Damit setzt die Hochschule einen nachhaltigen Akzent in der Ausbildung von qualifiziertem Nachwuchs für die Bundesverwaltung in ganz Deutschland. Die Bewerbungsfrist für das Folgesemester läuft derzeit. DataAgenda sprach mit Prof. Dr. Anna Schulze, Prof. Dr. Lorenz Franck und Marc Sahr aus dem DACS-Team.

DataAgenda: Frau Prof. Dr. Schulze, Sie sind als Informatikerin die wissenschaftliche Leiterin des Studienganges, was lernt man in diesem Studium?

Schulze**:** „Der Studiengang DACS ist ein dualer Studiengang, der zu 50 % aus Fächern der Informationstechnik besteht und zu 50 % aus Fächern des Verwaltungsmanagements. Unsere Absolventinnen und Absolventen werden maßgeblich bei der Digitalisierung der Bundesverwaltung mitwirken, sei es beispielsweise bei der Einführung der E-Akte, dem Betrieb von Bürgerportalen, der Abwehr von Cybersicherheitsrisiken oder der Kriminalitätsbekämpfung im Darknet.

DataAgenda: Digitalisierung ist also das Stichwort. Verfügt Ihre Hochschule in der Corona-Zeit nicht bereits selbst über einschlägige Erfahrung in der Digitalisierung?

Schulze: „Ja, die HS Bund hat im März dieses Jahres von heute auf morgen von Präsenzbetrieb auf digitale Fernlehre umgestellt. Dafür musste die schon vorhandene elektronische Lernplattform erheblich erweitert werden. Derzeit unterhalten wir einen Mischbetrieb: Zum Teil finden die Lehrveranstaltungen in virtuellen Kursräumen statt. Soweit es die aktuelle Corona-Lage zulässt, werden die Vorlesungen und Seminare vor Ort durchgeführt.“

DataAgenda: Unabhängig von virtuellen oder realen Kursräumen, wie verläuft das DACS-Studium insgesamt aus Sicht der Studierenden?

Schulze: „Das Studium umfasst drei Jahre. Vier theoretische Semester finden in Brühl statt. Im dritten und fünften Semester können die Studierenden ihre Kenntnisse in einer Bundesbehörde erproben. Abgeschlossen wird das Studium mit einer Abschlussarbeit.“

DataAgenda: Herr Prof. Dr. Franck, Sie sind der IT-Rechtler im Team. Wie vertragen sich Informatik und Recht im Studium überhaupt?

Franck**:** Wir verfolgen im neuen Studiengang konsequent einen interdisziplinären Ansatz. Auf der einen Seite ist nicht alles erlaubt, was technisch möglich ist. Auf der anderen Seite macht das Recht deutliche Vorgaben, was die Verwaltung im Digitalen aktiv zu leisten hat. Unsere Absolventinnen und Absolventen werden später direkt an der Schnittstelle beider Bereiche eingesetzt und müssen sich daher auch in beiden Bereichen zuhause fühlen.

DataAgenda: Unsere Leser sind naturgemäß am Datenschutzrecht besonders interessiert. Wie viel Datenschutz steckt denn im DACS?

Franck: Für das Datenschutzrecht sind in der Tat mehrere Lehrveranstaltungen vorgesehen. Nach einer Grundausbildung im aktuellen Europäischen Datenschutzrecht folgen aufbauende Veranstaltungen, beispielsweise zur Datenschutzorganisation oder zum bereichsspezifischen Datenschutzrecht der Sicherheitsbehörden. Wir verzahnen diese Themen eng mit Fragen des Informationssicherheitsrechts und des E-Government-Rechts.

DataAgenda: Herr Sahr, Sie sind als wissenschaftlicher Mitarbeiter insbesondere mit Organisationsfragen betraut. Wo liegt genau der Unterschied zu anderen „Cyber-Studiengängen“

Sahr: Unser Studiengang weist organisatorisch und inhaltlich einige Besonderheiten auf. Der DACS bildet für den öffentlichen Dienst aus. Das bedeutet, dass unsere Studierenden bereits an der Hochschule zu Beamtinnen und Beamten auf Widerruf ernannt werden. Damit ist natürlich auch ein Anwärtergehalt verbunden: Sie werden für das Studium bezahlt. Die Praktikumsphasen werden schon während des Studiums beim späteren Dienstherrn abgeleistet, Sie lernen also den Arbeitgeber schon sehr genau kennen. Da es sich bei den Praktikumsbehörden zum Teil um Sicherheitsbehörden handelt, ist ggf. eine sog. „Sicherheitsüberprüfung“ erforderlich. Thematisch bieten wir zum Ende des Studiums eine Spezialisierung in die namensgebenden Zweige „Digital Administration“ sowie „Cyber Security“. Sie können Sich also schon zu Beginn des Studiums festlegen, ob Ihnen eher die Verwaltungsaspekte oder die Sicherheitsaspekte mehr am Herzen liegen.

Das vollständige Interview können Sie hier nachlesen.

Abgrenzung von Verantwortlichem, Auftragsverarbeiter und gemeinsam Verantwortlichen

Was die Verantwortlichkeit für die Verarbeitung personenbezogener Daten angeht, kennt die DS-GVO im Wesentlichen drei Akteure. Zum einen den Verantwortlichen, der nach Art. 4 Nr. 7 DS-GVO als eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet und zum anderen den Auftragsverarbeiter. Der „Auftragsverarbeiter" wird als eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle definiert, der die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 4 Nr. 8 DS-GVO).

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.

Aktuell versucht der Europäische Datenschutzausschuss (EDSA) im Rahmen einer Konsultation zu diesem Thema eine noch klarere Abgrenzung für die Praxis zu finden. Dazu hat der EDSA einen Entwurf für eine Stellungnahme zur Abgrenzung von Verantwortlichem, Auftragsverarbeiter und gemeinsam Verantwortlichen veröffentlicht. Feedback erwartet der EDSA bis spätestens 19. Oktober 2020 unter Verwendung des bereitgestellten Formulars. Erst danach wird eine finale Version des Dokuments veröffentlicht werden.

Quelle: European Data Protection Board

LDI NRW möchte Verhaltensregeln nach Art. 40 DS-GVO fördern

Nach ErwG 98 der DS-GVO sollen Verbände oder andere Vereinigungen, die bestimmte Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, ermutigt werden, in den Grenzen dieser Verordnung Verhaltensregeln auszuarbeiten, um eine wirksame Anwendung der DS-GVO zu erleichtern. Dabei soll den Besonderheiten der in bestimmten Sektoren erfolgenden Verarbeitungen und den besonderen Bedürfnissen der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen Rechnung getragen werden.

Verhaltensregeln nach Artikel 40 DS-GVO bieten die Möglichkeit, ein Regelwerk festzulegen, das zur ordnungsgemäßen Anwendung der DS-GVO auf praktische, transparente und potenziell kosteneffiziente Weise beiträgt. Sie berücksichtigen die Besonderheiten eines bestimmten Sektors beziehungsweise seiner Verarbeitungstätigkeiten. Dabei können auch die besonderen Bedürfnisse von Kleinst-, Klein- und Mittelbetrieben Berücksichtigung finden.

Um dieses noch nicht rege genutzte Instrument und die Möglichkeit der Etablierung von Verhaltensregeln zu fördern, bietet die LDI NRW sowohl ein neuen Antragsformular zur Genehmigung von Verhaltensregeln sowie eine Checkliste von Genehmigungsvoraussetzungen.
Die Aufsichtsbehörde sieht die Checkliste als eine Arbeitshilfe. Sie soll Antragstellerinnen und Antragstellern die Vorbereitung und Prüfung ihrer Unterlagen und die Kommunikation mit der Aufsichtsbehörde erleichtern. Auch die Prüfung der Aufsichtsbehörde soll damit unterstützt und beschleunigt werden können. Rückmeldungen und Beratungen können sich dann auch an der Checkliste orientieren, so dass die Kommunikation vereinfacht wird.

Quelle: LDI NRW

Code of Conduct für die Pseudonymisierung geplant

Die Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. gibt bekannt, dass sie in Kooperation mit dem Digitalverband Bitkom EU-weite Verhaltensregeln für Pseudonymisierungen in der Datenverarbeitung etablieren möchte. Grundlage dafür sei der im Rahmen des Digital-Gipfels 2019 entwickelte Entwurf der Fokusgruppe Datenschutz für einen Code of Conduct.

Im Rahmen des Digital-Gipfels 2019 wurde unter Leitung von Prof. Dr. Rolf Schwartmann, Vorstandsvorsitzender der GDD, durch Experten der Fokusgruppe Datenschutz ein Entwurf für einen Code of Conduct für die Pseudonymisierung personenbezogener Daten erarbeitet.
GDD und Bitkom sehen in der Pseudonymisierung enormes Potenzial, datenschutzkonforme Datenverarbeitung zu ermöglichen und gleichzeitig die Rechte und Interessen von Betroffenen angemessen zu schützen. Betreiber von Plattformen und andere Datenverarbeiter sollen die Möglichkeit erhalten, Pseudonymisierungen anhand transparenter und möglichst einheitlicher Vorgaben vorzunehmen.
Ziel der gemeinsamen Initiative der Verbände ist die Erarbeitung eines Code of Conducts gem. Art. 40 DS-GVO, der durch eine Datenschutzaufsichtsbehörde genehmigt wird.

Weitere Informationen zum Projekt „Code of Conduct Pseudonymisierung“ sowie den *„Entwurf für einen Code of Conduct zum Einsatz DS-GVO konformer Pseudonymisierung“* in der Version 1.0 finden Sie auf den Seiten der GDD (https://www.gdd.de/projekte/code-of-conduct-pseudonymisierung-1).

>> Die vollständige Pressemitteilung können Sie hier abrufen.

Leitlinien zur Körpertemperaturmessung veröffentlicht

Bereits zu Beginn der Corona-Pandemie wurde die Frage diskutiert, welche Maßnahmen Arbeitgeber zur Eindämmung der Pandemie und unmittelbar auch zur Aufrechterhaltung der betrieblichen Tätigkeit umsetzen können. In diesem Zusammenhang stellte sich auch oftmals die Frage, ob Arbeitgeber im Rahmen von Zugangskontrollen Fiebermessungen an ihren Beschäftigten vornehmen dürfen.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit aus Rheinland-Pfalz äußerte sich kritisch zu dieser Fragestellung und kam im Ergebnis zu der Feststellung, dass eine verpflichtende Fiebermessung der Mitarbeiter als Zugangskontrolle unzulässig sei. Nach Auffassung der Aufsichtsbehörde fehle es insbesondere an der notwendigen Erforderlichkeit der Fiebermessung.

Nach Art. 9 Abs. 2 lit. b DS-GVO i.V.m. § 26 Abs. 3 BDSG sei die Verarbeitung besonderer Kategorien personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses unter anderem zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht erforderlich sei und kein Grund zu der Annahme bestehe, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen.

Die Aufsichtsbehörde ging davon aus, dass die reine Tatsache, dass eine erhöhte Körpertemperatur zu verzeichnen ist, noch nicht automatisch den Schluss auf das Vorliegen einer Corona-Erkrankung zulasse. Umgekehrt müsse sich eine bereits bestehende Corona-Erkrankung nicht zwangsläufig durch eine erhöhte Körpertemperatur zu erkennen geben. Daher zweifelte die Aufsichtsbehörde sogar bereits an der Geeignetheit der Körpertemperaturmessung.

Nun hat sich auch der Europäische Datenschutzbeauftragte mit der Thematik beschäftigt und stellt seine Auffassung als Leitlinie zur Körpertemperaturmessung der Öffentlichkeit zur Verfügung.
Eine der wesentlichen Feststellung des Europäischen Datenschutzbeauftragten dürfte sein, dass lediglich manuelle Messungen, bei denen keine nachfolgende Speicherung, Registrierung erfolgen, nicht vom Anwendungsbereich des europäischen Datenschutzrechts erfasst würden.

Ferner enthält die Leitlinie die Empfehlung, dass verpflichtende Temperaturkontrollen nicht ausschließlich auf einer automatisierten Verarbeitung ohne jegliche menschliche Beteiligung beruhen sollten.

Abgerundet wird das Papier durch eine nicht abschließende Liste von technischen und organisatorischen Empfehlungen, die gebührend berücksichtigt werden sollten, um sicherzustellen, dass angemessene Sicherheitsvorkehrungen vorhanden sind sowie spezifische Empfehlungen für die nötige Transparenz gegenüber den betroffenen Personen eingehalten wird.

Quelle: European Data Protection Supervisor

Studie zum Datenschutz-Einwilligungsmanagement

Art. 4 Nr. 11 DS-GVO definiert die Einwilligung als „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist." Die Einwilligung ist daher einerseits Betroffenenrecht, da sie der betroffenen Person die Möglichkeit gibt, aktiv über die Verarbeitung, ihre Zwecke und näheren Umstände zu bestimmen. Andererseits ist sie aus Sicht des Verantwortlichen ein vollgültiger Erlaubnistatbestand im Sinne von Art. 6 Abs. 1 lit. a DS-GVO. Mittels einer Einwilligung können ggf. Verarbeitungen gerechtfertigt werden, die allein auf Grundlage der gesetzlichen Tatbestände ausgeschlossen wären.

Gemäß den Vorgaben der DS-GVO muss eine Einwilligung informiert, differenziert und freiwillig erfolgen. Um diese Anforderungen sowohl rechtssicher als auch nutzerfreundlich umzusetzen, sind Einwilligungsmanagement-Systeme (EMS) nötig.

Das Bundesministerium der Justiz und für Verbraucherschutz hat das Forschungsprojekt „Innovatives Datenschutz-Einwilligungsmanagement" mit dem Ziel in Auftrag gegeben, bestehende Einwilligungsmanagement-Modelle zu analysieren, Nutzerpräferenzen zu erfassen und neue Lösungsansätze zur rechtskonformen und nutzerfreundlichen Datenschutz-Einwilligung zu entwickeln. Das zentrale Ergebnis der Studie ist, dass es Möglichkeiten gibt, die Vorgaben der Datenschutz-Grundverordnung sowohl rechtskonform als auch nutzerfreundlich in der Praxis umzusetzen. Dazu wird für den Online-Bereich ein innovatives Best Practice-Modell mit einem konkreten Web-Design vorgestellt. Der Projektbericht beschreibt sowohl die zentralen Anforderungen an das Best Practice-Modell als auch Schritte zur Umsetzung.

Quelle: Bundesministerium der Justiz und für Verbraucherschutz