Datenschutz newsbox

Ausgabe 2 2018

DATAKONTEXT

Editorial

Die Medienpräsenz von Volkswagen war und ist in jüngster Vergangenheit beachtlich gewesen. Nach dem das Image durch den Skandal mit manipulierten Abgaswerten einigermaßen ramponiert war, wurde das Ansehen durch weitere „Abgastests“an Affen und Menschen noch mehr in Leidenschaft gezogen. Für weiteren Ärger bei Volkswagen sorgte das „Projekt Schutzranzen“. Über eine App auf dem Smartphone des Kindes beziehungsweise über einen GPS-Tracker im jeweiligen Rucksack sollte die Position von Grundschulkindern ständig in die „Schutzranzen-Cloud“ übermittelt werden. Für den Fall, dass ein Kind im Straßenverkehr nun in die Nähe eines Autos kommt, sollte der Fahrer, der ebenfalls eine App installiert hat oder über das „Onboard-System im Auto von morgen“ verfügt, akustisch gewarnt werden. Die meisten Eltern und Lehrer waren not amused.

Ebenfalls einem Traum von Hardcore-Helikopter-Eltern scheint ein anderes Projekt aus Indien entsprungen zu sein. Die Regierung im indischen Delhi will Eltern über eine App Zugriff auf vorgesehene Videoüberwachung der Klassenzimmer in öffentlichen Schulen gestatten. Die App soll auch mit einer Beschwerde-Funktion für die Eltern ausgestattet werden. Müßig zu erwähnen, dass autorisierten Beamten des Bildungsministeriums ebenfalls jederzeit Zugriff auf das Überwachungssystem gewährt werden soll.

Beruhigend ist, dass es diese Zustände in Deutschland (noch) nicht gibt. Ganz im Gegenteil ist das Datenschutz-Niveau in Deutschland anscheinend derart hoch, dass davon auszugehen ist, dass weite Teile der Bevölkerung aus „Datenschutzgründen“ im Falle eines atomaren Erstschlags nicht „vorgewarnt“ werden können.

Persönlichkeitsrechten drohen jedoch auch von anderer Stelle Gefahren. Bald könnten Unbeteiligte „Darsteller“ in sog. Fake-Pornos werden. Verbesserte KI-Technologien machen es möglich! Ob das Durchforsten bekannter Porno-Portale nach dem eigenen Konterfei eine sinnvolle Gegenmaßnahme darstellt, darf bezweifelt werden, fürchtet

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

Transparenzpflichten bei der Datenverarbeitung – Praxishilfe aktualisiert

Art. 13 DS-GVO widmet sich den Informationspflichten bei der Direkterhebung, Art. 14 ist das Pendant bei Erhebung von Daten bei Dritten. Bei der Umsetzung der neuen Vorschriften stellen sich zahlreiche Einzelfragen.

Der GDD-Arbeitskreis „DS-GVO-Praxis“ stellte bereits seine Hybrid-Datenschutzinformation vor, welche den jeweiligen Anforderungen der Artt. 13 & 14 DS-GVO gleichermaßen gerecht werden soll. Daneben werden zahlreiche Einzelfragen beantwortet.

In Version 2.0 werden die Ausführungen der Artikel-29-Datenschutzgruppe zu den Transparenzpflichten berücksichtigt. Zu den vertieften Themen gehören die Frage des Medienbruchs, der Bestandsinformation („Transparenz-Reset") und der regelmäßigen Wiederholung.

GDD-Praxishilfe DS-GVO VII – Transparenzpflichten bei der Datenverarbeitung, Version 2.0, Stand Januar 2018

https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_7.pdf

Die GDD veröffentlicht Praxishinweise für Auftragsverarbeiter nach Art. 28 DS-GVO

Art. 28 DS-GVO stellt die zentrale Norm für die Auftragsverarbeitung dar. Beteiligte einer Auftragsverarbeitung sind der Verantwortliche und der Auftragsverarbeiter. „Verantwortlicher“ ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Abs. 7 DS-GVO). „Auftragsverarbeiter“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 4 Abs. 8 DS-GVO). Gem. Art. 4 Abs. 10 DS-GVO ist die Auftragsverarbeitung weiterhin dergestalt privilegiert, dass der Auftragsverarbeiter kein Dritter ist. Eine Beschränkung der Privilegierung auf den EWR-Raum erfolgt nicht. Auftragsverarbeiter im Drittland sind damit ebenfalls keine „Dritten“ für den Verantwortlichen. Während die Norm teilweise bekannte Vorgaben an die Dienstleisterauswahl und die vertragliche Gestaltung stellt, enthält die DS-GVO an verschiedenen Stellen eigene Rechtspflichten für Auftragsverarbeiter.

Diese Praxishinweise der GDD möchten Hilfestellungen für Auftragsverarbeiter geben, wie die gesetzlichen Vorgaben umgesetzt werden können.

Praxishinweise für Auftragsverarbeiter nach Art. 28 DS-GVO
(Version 1.0, Stand Februar 2018)
https://www.gdd.de/downloads/praxishilfen/GDD- Hinweise_fuer_Auftragsverarbeiter_Art._28_v1.0.pdf

Linksammlung zum Thema DS-GVO

Seit In-Kraft-Treten der DS-GVO bis zum heutigen Tage sind bereits zahlreiche Fachaufsätze, Working Paper, Praxisleitfäden, Kurzpapiere und diverse weitere Literatur erschienen, die sich mit dem Thema der DS-GVO allgemein, mit konkreten Einzelfragen oder mit der Umsetzung der DS-GVO befassen.

Die Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS) e.V. pflegt auf ihrem Internetauftritt eine Linksammlung zum Thema, die die bisher erschienen Publikationen in einer übersichtlichen Liste aufführt. Die Liste ist bereits untergliedert in Rubriken wie „Zeitschriften“ und „Praxishilfen“. Alle Publikation sind, sofern diese öffentlich im Netz zugänglich sind, mit dem Dokument verlinkt.

Die Linksammlung dürfte für die meisten eine gute Anlaufstelle bei der Beschäftigung mit dem Thema DS-GVO darstellen.

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS) e.V.

Adressdaten ohne Einwilligung: Kaufvertrag insgesamt nichtig

Das OLG erklärt den Verkauf von Adressdaten wegen fehlender Einwilligung nach dem Bundesdatenschutzgesetz (BDSG) für unwirksam und weist Ansprüche trotz vertragswidriger Nutzung durch Dritte für anstößige Werbe-E-Mails zurück.

Die Klägerin handelt mit Adressdaten. Sie nimmt den beklagten Insolvenzverwalter der vormals ebenfalls mit Adressdaten handelnden Schuldnerin auf Schadensersatz und Unterlassen in Anspruch. Der Geschäftsführer der Klägerin war zuvor Geschäftsführer der Schuldnerin. Er hatte am Tag der Insolvenzeröffnung vom Beklagten verschiedene Internet-Domains einschließlich der über diese generierten Adressen für 15.000 € gekauft. Die Daten befanden sich ursprünglich auf zwei Servern der Schuldnerin und wurden auf einem USB-Stick übergeben. Die Server selbst, auf denen die Daten weiterhin rekonstruierbar lagen, wurden vom Beklagten an eine ebenfalls mit Adressen handelnde dritte Firma verkauft. Diese nutzte nach dem Vertrag der Klägerin rund eine Million Adressen, um Werbe-E-Mails für die Internetseite sexpage.de zu versenden.

Das Landgericht hat der Klage stattgegeben. Die hiergegen gerichtete Berufung des Beklagten hatte vor dem OLG Erfolg. Der Klägerin, so das OLG, stünden keinerlei vertragliche Ansprüche zu. Der Kaufvertrag sei vielmehr insgesamt nichtig, da die Adressinhaber in den Verkauf ihrer Daten nicht wirksam eingewilligt hätten. Der Vertrag verstoße gegen die Vorgaben des BDSG. Die Nutzung sogenannter personenbezogener Daten sei nur zulässig, wenn der Betroffene einwillige oder das so genannte Listenprivileg greife. „Name, Postanschrift, Telefonnummer und E-Mail-Adresse einer Person“ stellten „klassische“ personenbezogene Daten dar. Auch der einmalige Verkauf derartiger Daten – wie hier – unterfalle dem Adresshandel im Sinne von § 28 Abs. 3 S. 1 BDSG. Das so genannte Listenprivileg nach § 28 Abs. 3 S. 2 BDSG greife nicht, da es sich nicht um „zusammengefasste Daten von Angehörigen einer bestimmten Personengruppe“ handele.

Eine Einwilligung nach dem BDSG sei, betont das OLG, „nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht, der auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie (...) auf die Folgen der Verweigerung der Einwilligung“ hingewiesen wird. Sie müsse grundsätzlich schriftlich abgegeben werden. Außerdem sei sie „besonders hervorzuheben“, wenn sie – wie hier – zusammen mit anderen Erklärungen erteilt werde. Nach dem von der Klägerin selbst vorgetragenen Wortlaut der Einwilligungserklärung seien jedoch weder die betroffenen Daten noch Kategorien etwaiger Datenempfänger oder der Nutzungszweck – Adresshandel – konkret genug bezeichnet worden. Es fehle zudem die erforderliche Hervorhebung.

Der Vertrag verpflichte die Parteien darüber hinaus „systematisch“ zu einem unlauteren wettbewerbswidrigen Verhalten, so dass auch deshalb von einer Gesamtnichtigkeit auszugehen sei. Die Zusendung von Werbe-E-Mails ohne Einwilligung stelle eine unzumutbare Belästigung nach § 7 Abs. 2 Nr. 3 UWG dar.

Das Urteil ist nicht rechtskräftig; die Klägerin kann Nichtzulassungsbeschwerde beim Bundesgerichtshof einlegen.

Oberlandesgericht Frankfurt am Main, Urteil vom 24.01.2018, Az. 13 U 165/16

Beispiel zur Durchführung einer Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung (DSFA) soll gem. Art. 35 DS-GVO eine umfassende Risikobewertung von Datenverarbeitungsvorgängen ermöglichen. Sie ersetzt die bisherige Vorabkontrolle nach § 4d Abs. 5 BDSG a.F., wobei beide Instrumente nicht in allen Teilen vollständig deckungsgleich sind.

Der Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter – Privacyofficers.at – hat nun ein praxistaugliches Beispiel zur Durchführung einer DSFA zum Download bereitgestellt. Erklärtes Ziel der Autoren ist es, diese Umsetzungshilfe aktuell zu halten. In der vorliegenden Version wurde das österreichische Datenschutz-Anpassungsgesetz 2018 entsprechend berücksichtigt.

Das vorliegende Durchführungsbeispiel gibt einen Überblick und praxistaugliche Informationen über die Durchführung einer DSFA am Beispiel einer Videoüberwachung inkl. Risikobewertung aus Sicht der Betroffenen. Die Autoren verstehen das Durchführungsbeispiel nur als Orientierungshilfe, in der wichtigsten Inhalte der DSGVO bezüglich der Durchführung einer DSFA in kompakter und übersichtlicher Form zusammenfasst werden.

Link zum Download

Auflösung: Datenschutz-Quiz der GDD zum Europäischen Datenschutztag

Zum 12. Europäischen Datenschutztag veranstaltete die GDD einen Datenschutz-Quiz. In diesem Jahr hatten die Teilnehmer die Gelegenheit, ihr Wissen zur DS-GVO unter Beweis zu stellen. Zu gewinnen gab es 50 großformatige Textkunst-Poster (140x100cm) mit dem englischen Text der DS-GVO im Design der Europaflagge. Die Gewinner stehen nunmehr fest, so dass im Nachgang auch die richtigen Antworten veröffentlicht werden.

Hier nun die Auflösung der Quizfragen:

Frage 1:
Innerhalb welcher Frist müssen Verletzungen des Schutzes personenbezogener Daten möglichst gemeldet werden?
Antwort:
72 Stunden. Gem. Art. 33 Abs. 1 DS-GVO meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde.

Frage 2:
Müssen die Kontaktdaten des/der Datenschutzbeauftragen der Aufsichtsbehörde mitgeteilt werden?
Antwort:
Ja. Der Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten ab dem 25. Mai 2018 und teilt diese Daten gem. Art. 37 Abs. 7 DS-GVO der Aufsichtsbehörde mit.

Frage 3:
Mit einem Bußgeld bis zu welcher Höhe ist das Fehlen eines Vertrages zur Auftragsverarbeitung nach der DS-GVO bedroht?
Antwort:
10 Millionen Euro oder im Fall eines Unternehmens bis zu 2% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs. Der pflichtwidrige Verzicht auf einen Vertrag stellt einen Verstoß gegen Art. 83 Abs. 4 lit. a iVm Art. 28 DS.GVO dar.

Frage 4:
Ist für die Einwilligung der betroffenen Person zwingend die Schriftform vorgesehen?
Antwort:
Nein. Weder Art. 4 Nr. 11 noch Art. 7 DS-GVO machen die wirksame Einwilligung von der Schriftform abhängig.
Erwägungsgrund 32 führt aus, dass die Erklärung ggf. elektronisch oder mündlich erfolgen kann, bzw. durch Anklicken eines Kästchens beim Besuch einer Internetseite u.s.w. Hauptsache, der Nachweis ist gewährleistet. (Besonders aufmerksame Teilnehmer verwiesen auf das Schriftformerfordernis des § 26 Abs. 2 Satz 3 BDSG 2018. Doch selbst hiervon kann abgewichen werden, wenn wegen besonderer Umstände eine andere Form angemessen ist.)

Frage 5:
Darf ein Auftragsverarbeiter zur Aufgabenerfüllung Subunternehmer einsetzen?
Antwort:
Grundsätzlich ja. Es müssen allerdings die Voraussetzungen des Art. 28 Abs. 2 und 4 DS-GVO eingehalten sein. (Wer hier unter Verweis auf Art. 28 Abs. 2 Satz 1 DS-GVO zunächst auf „ nein" getippt hat, lag ebenfalls richtig; es kommt wie immer auf die Begründung an.)

CNIL überarbeitet DSFA-Tool

Die Commission Nationale de l'Informatique et des Libertés (CNIL; deutsch Nationale Kommission für Informatik und Freiheiten), die nationale Datenschutzbehörde Frankreichs mit Sitz in Paris, hat bereits vor geraumer Zeit eine Software für die Durchführung einer sog. Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO veröffentlicht.

Die sog. PIA-Software (Privacy Impact Assessment) ist Teil eines Prozesses zur Unterstützung der für die Verarbeitung Verantwortlichen bei der Umsetzung der Pflichten aus der DS-GVO. Das Tool ist in französischer und englischer Sprache verfügbar und soll die Datenschutz-Folgenabschätzung erleichtern und die Verantwortlichen bei der Durchführung einer Datenschutz-Folgenabschätzung begleiten, die ab Mai 2018 für einige Verarbeitungen obligatorisch wird. Dieses Instrument zielt auch darauf ab, die von der CNIL veröffentlichten Leitfäden zum Thema Datenschutz-Folgenabschätzung zu erleichtern.

Das Tool richtet sich vor allem an Verantwortliche, die mit dem PIA-Ansatz nicht vertraut sind. Es handelt sich um eine „ ready to use" -Version, die einfach auf einem Rechner gestartet werden kann. Das Tool wird auch in einer sog. portable-Version angeboten, die keiner Installation bedarf. Es soll auch möglich sein, das Tool auf Servern einzusetzen, um es in bereits intern in Unternehmen eingesetzte Tools zu integrieren.

Verantwortliche können den Inhalt des Tools an ihre spezifischen Bedürfnisse oder Ihren Tätigkeitsbereich anpassen, indem sie beispielsweise ein DSFA-Modell erstellen, welches dupliziert und für ähnliche Behandlungen verwendet werden kann. Außerdem gestattet es die Lizenz, den Quellcode des Tools zu modifizieren, um Funktionalitäten hinzuzufügen oder es in bereits intern veröffentlichte Tools zu integrieren.

In der überarbeiteten Version steht sowohl eine französische als auch eine englische Sprachfassung zur Verfügung. Interessierte können sich an die grundlegenden Funktionen der Software mit Hilfe eines Youtube-Videos herantasten.

Das Tool kann mit folgenden Betriebssystemen betrieben werden:
- Windows (32 and 64 bits)
- Linux (32 bits)
- Linux (64 bits)
- Mac OS

CNIL
https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

Anleitung zur Erstellung eines IT-Grundschutz-Profils

Bei der Modernisierung des IT-Grundschutzes wurde neben den neuen Vorgehensweisen und dem IT-Grundschutz-Kompendium auch ein Konzept zu IT-Grundschutz-Profilen eingeführt. Ziel der IT-Grundschutz-Profile ist es, dass zunächst eine Institution oder Branche den IT-Grundschutz zielgenau auf ihre individuellen Sicherheitsanforderungen anpasst und die Ergebnisse anschließend als Schablone von anderen Institutionen mit vergleichbaren Sicherheitsanforderungen oder IT-Umgebungen adaptiert werden können. Dazu veröffentlicht das BSI nun mit der „Strukturbeschreibung für IT-Grundschutz-Profile" eine Anleitung zur Erstellung eines IT-Grundschutz-Profils, die die Anwender durch den gesamten Profilprozess führt. Mögliche Anwendungsbereiche für Profile sind zum Beispiel Kommunalverwaltungen, Krankenhäuser oder Wasserwerke im Bereich der Kritischen Infrastrukturen.

Die Strukturbeschreibung steht als Community Draft auf der IT-Grundschutz-Webseite zur Verfügung. Mehrere Anwendergruppen haben bereits begonnen, spezifische IT-Grundschutz-Profilen zu erstellen. Das BSI tauscht sich mit diesen Anwendergruppen aus, um so den generellen Aufbau von IT-Grundschutz-Profilen weiterzuentwickeln. Hierüber hinaus wurde eine Masterarbeit erstellt, die sich näher mit IT-Grundschutz-Profilen beschäftigt und von deren Ergebnissen interessierte Anwender partizipieren können.

Bundesamt für Sicherheit in der Informationstechnik
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzProfile/itgrundschutzProfile_node.html

Datenschutz newsbox

EU-Kommission veröffentlicht Leitfaden zu neuen Datenschutzbestimmungen

Die Kommission veröffentlicht einen Leitfaden zu den neuen, ab 25.Mai 2018 geltenden Datenschutzbestimmungen, um deren reibungslose Anwendung in der gesamten EU zu erleichtern. Ergänzend dazu stellt sie ein neues Online-Tool für kleine und mittlere Unternehmen ins Netz.

Knapp 100 Tage vor Geltungsbeginn der neuen Bestimmungen gibt der Leitfaden einen Überblick darüber, was die Europäische Kommission, die nationalen Datenschutzbehörden und die nationalen Behörden noch tun sollten, um die Vorbereitungen erfolgreich abzuschließen.

Zwar schafft die neue Verordnung ein einheitliches und unmittelbar in allen Mitgliedstaaten anwendbares Regelwerk, sie erfordert jedoch in bestimmten Bereichen weitreichende Anpassungen, darunter Änderungen an bestehenden Gesetzen durch die Regierungen der Mitgliedstaaten und Einrichtung des Europäischen Datenschutzausschusses durch die Datenschutzbehörden. Der Leitfaden enthält die wichtigsten Neuerungen und zeigt Chancen auf, die sich aus den neuen Bestimmungen ergeben; zudem gibt er einen Überblick über die geleisteten Vorarbeiten und hält fest, was vonseiten der Europäischen Kommission sowie der Datenschutzbehörden und Regierungen der Mitgliedstaaten noch zu tun ist.

Informationen:
Leitfaden der Kommission

Fragen und Antworten

Online-Tool

Einwilligung und Transparenz nach der DS-GVO

Am 28. November 2017 verabschiedete die Artikel-29-Datenschutzgruppe die Working Paper 259 und 260 zu den Themen Einwilligung und Transparenz. Die Papiere sind ein wichtiger Schritt hin zu mehr Rechtssicherheit, harren allerdings noch der Finalisierung. Die GDD hat im Rahmen der öffentlichen Konsultation entsprechende Stellungnahmen abgegeben.

WP 259 - Guidelines on Consent under Regulation 2016/679
Beim Übergang zum neuen Datenschutzrecht ist u.a. wesentlich, wie mit Alteinwilligungen umgegangen wird. Nach Auffassung der GDD sind sämtliche Einwilligungen, die unter der Datenschutzrichtlinie 95/46/EG wirksam abgegeben wurden, auch künftig gültig. Es besteht zudem keine Notwendigkeit, die Einwilligung regelmäßig aufzufrischen, wenn sie einmal Wirksamkeit erlangt hat.

Die GDD-Stellungnahme zum WP 259 in englischer Sprache finden Sie hier.

WP 260 - Guidelines on Transparency under Regulation 2016/679
Die Unterscheidung der Transparenzpflichten nach Artt. 13 und 14 DS-GVO richtet sich danach, ob die Daten direkt beim Betroffenen erhoben werden. Für die Direkterhebung kann die reine Beobachtung jedoch nicht ausreichen. Es kommt aus Sicht der GDD auch darauf an, dass die betroffene Person Kenntnis von der Erhebung hat.

In WP 260 wird vorgeschlagen, die Transparenzinformationen regelmäßig aufzufrischen, auch wenn sich inhaltlich nichts geändert hat. Ein solches Vorgehen wirkt jedoch kontraproduktiv und führt zu sog. „ transparency fatigue". Darüber hinaus fordert die DS-GVO keine Bestandsinformation an sämtliche Betroffenen (sog. Transparenz-Reset) am 25. Mai 2018.
Ein Medienbruch innerhalb derselben Information muss möglich bleiben. Viele Verarbeitungssituationen lassen es nicht zu, der betroffenen Person einen mehrseitigen Abdruck der Transparenzinformationen unmittelbar zur Verfügung zu stellen (z.B. Automatenverkauf, Telefongeschäfte, Postkarte für Gewinnspiel).

Und schließlich ist die GDD der Überzeugung, dass es auch im Rahmen der Direkterhebung gem. Art. 13 DS-GVO Fälle geben kann, in denen die Mitteilung von Transparenzinformationen unmöglich ist, selbst wenn der Unionsgesetzgeber dies ausdrücklich nur in Art. 14 DS-GVO berücksichtigt hat.
Die GDD-Stellungnahme zum WP 260 in englischer und deutscher Sprache finden Sie hier.

Meldeformular Datenschutzbeauftragter gem. Art. 37 Abs. 7 DS-GVO

Die EU-Mitgliedsstaaten haben die Möglichkeit, die Pflicht zur Benennung eines DSB in ihren nationalen Ausführungsgesetzen auf weitere Stellen auszudehnen (Art. 37 Abs. 4 S. 1 DS-GVO). Der Bundesgesetzgeber hat diesen Regelungsspielraum genutzt, um die Pflicht zur Benennung von betrieblichen Datenschutzbeauftragten dem in Deutschland bestehenden „Status quo" anzupassen (vgl. § 4f BDSG-alt sowie § 38 BDSG-neu). Das Kurzpapier Nr. 12 – Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern – verweist auf die Pflicht, die Kontaktdaten des DSB nach Art. 37 Abs. 7 DS-GVO zu veröffentlichen und der Aufsichtsbehörde mitzuteilen. Es wird darauf hingewiesen, dass die Aufsichtsbehörden den mitteilungspflichtigen Stellen ein Formular zur Mitteilung der Kontaktdaten des DSB zur Verfügung stellen werden.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz hat bereits ein solches Meldeformular gem. Art. 37 Abs. 7 DS-GVO online gestellt. Das Formular soll der Mitteilung der Kontaktdaten der oder des Datenschutzbeauftragten eines für die Verarbeitung Verantwortlichen an die Aufsichtsbehörde auf Grundlage des Art. 37 Abs. 7 der Europäischen Datenschutz-Grundverordnung dienen. Es wird jedoch explizit betont, dass dieses Formular ausschließlich Testzwecken dient und noch NICHT für eine Meldung nach Art. 37 (7) DS-GVO genutzt werden kann. Sofern Interessierte vor dem 25. Mai 2018 Kontaktdaten des/der Datenschutzbeauftragten an den Landesbeauftragten melden möchten, wird um eine entsprechende Mail an poststelle(at)datenschutz.rlp.de gebeten.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

Datenschutzkonferenz veröffentlicht Kurzpapier zur Auftragsverarbeitung

Zur Anpassung der Datenschutzorganisation an die neuen Anforderungen der DS-GVO gehört unter anderem die Überprüfung bestehender Vertragsverhältnisse sowie die Anpassung der Vertragsmuster für zukünftige Outsourcing-Dienstleistungen. Für den Bereich der Auftragsverarbeitung sind viele Einzelfragen noch in der Diskussion, sei es die Abgrenzung zur Funktionsübertragung oder zur gemeinsamen Verantwortlichkeit, das Fortbestehen der bisherigen Privilegierung von Auftragsverhältnissen oder schlicht die Anwendung auf Fernwartungsvorgänge. Diese Fragen müssen durch Wissenschaft und Praxis und insbesondere durch den noch zu konstituierenden Europäischen Datenschutzausschuss befriedigend gelöst werden.

Wie schon bislang besteht auch unter der DS-GVO eine Sonderregelung für Verarbeitungen von personenbezogenen Daten im Auftrag. Allerdings legt die DS-GVO den Auftragsverarbeitern künftig mehr Verantwortung und mehr Pflichten auf. Nach Art. 29 DS-GVO ist der aufgrund eines Auftrages tätige Dienstleister weisungsgebunden. Er führt daher die Verarbeitung für den Auftraggeber nicht als Dritter i. S. d. Art. 4 Nr. 10 DS-GVO durch. Es besteht vielmehr zwischen dem den Auftrag erteilenden Verantwortlichen und seinem Auftragsverarbeiter ein „Innenverhältnis". Die Verarbeitung durch den Auftragsverarbeiter wird deshalb grundsätzlich dem Verantwortlichen zugerechnet. Zu beachten ist, dass die Datenverarbeitung im Auftrag auch künftig keine Erlaubnis darstellt, Daten dem Auftragsverarbeiter zu offenbaren, die aufgrund gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, vertraulich zu behandeln sind (vgl. § 1 Abs. 2 S. 3 BDSG-neu).

Die sog. Datenschutzkonferenz hat zum Thema Datenverarbeitung im Auftrag das „Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO" veröffentlicht und ersetzt damit das BayLDA-Kurzpapier Nr. 10 zum Thema. Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

BayLDa

Hamburgisches Datenschutzgesetz konkretisiert europäische Regelungen

Das Hamburgische Datenschutzgesetz sichert das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger gegenüber den öffentlichen Stellen in Hamburg. Gleichzeitig stellt es aber auch die zentrale und unerlässliche Rechtsgrundlage für die Hamburgische Verwaltung dar, um zur Erfüllung ihrer unterschiedlichen Aufgaben Daten zu verarbeiten. Die Normen des Hamburgischen Datenschutzgesetzes garantieren daher individuelle Rechte ebenso wie sie den rechtsstaatlichen Ablauf der Verwaltung insbesondere beim Erheben, Speichern und Übermitteln von personenbezogenen Daten sicherstellen.
Das Hamburgische Datenschutzgesetz, das der Senat am 16.01.2018 vorgelegt hat, berücksichtigt nun die Entwicklungen in Bezug auf die DS-GVO konkretisiert die europäischen Regelungen für den Umgang mit personenbezogenen Daten durch Behörden, Verwaltung und andere öffentliche Stellen.
Hierzu erklärt Justizsenator Dr. Till Steffen: „Personenbezogene Daten sind eine zentrale Ressource des digitalen Zeitalters. Mit der Datenschutzgrundverordnung und dem Hamburgischen Datenschutzgesetz ist es gelungen, die Interessen von Wirtschaft und Verwaltung in Einklang mit dem Recht auf informationelle Selbstbestimmung zu bringen. Für den Datenschutz ist das ein Meilenstein. Bürgerinnen und Bürger bekommen die Hoheit über ihre Daten zurück und Unternehmen und Verwaltung haben einen klaren Rahmen. Hervorzuheben ist, dass wir dieses Plus an Datenschutz durch weniger Gesetzestext erreichen."

Hamburg.de

Vereinigtes Königreich gilt ab dem 30.03.2019 als Drittland

Die Europäische Kommission teilt in einer Pressemitteilung vom 9. Januar 2018 mit, dass das Vereinigte Königreich ab dem 30.03.2019 als sog. Drittland einzustufen sein wird. Dies ist die Konsequenz der Erklärung des Vereinigten Königreichs gem. Artikel 50 des Vertrags über die Europäische Union aus der Union auszutreten. Diese bedeutet, dass das gesamte Primär- und Sekundärrecht der Union für das Vereinigte Königreich ab dem 30. März 2019, 00:00 Uhr (MEZ) („Rücktrittsdatum") nicht mehr anwendbar ist, es sei denn, ein ratifiziertes Rücktrittsabkommen legt einen anderen Zeitpunkt fest.

Angesichts der erheblichen Unsicherheiten, insbesondere hinsichtlich des Inhalts einer möglichen Rücknahmevereinbarung, werden alle Beteiligten, die personenbezogene Daten verarbeiten, an die rechtlichen Auswirkungen erinnert, die zu berücksichtigen sind, wenn das Vereinigte Königreich ein Drittland wird.

Vorbehaltlich etwaiger Übergangsregelungen, die in einem möglichen Rücktrittsabkommen enthalten sein können, gelten ab dem Rücktrittsdatum die EU-Vorschriften für die Übermittlung personenbezogener Daten in Drittländer. Abgesehen von einer „ Angemessenheitsentscheidung", die den freien Verkehr personenbezogener Daten aus der EU ermöglicht, ohne dass der EU-Datenexporteur zusätzliche Garantien einführen muss oder weiteren Bedingungen unterliegt, erlauben die EU-Datenschutzvorschriften (sowohl nach der aktuellen Richtlinie 95/46 als auch der Datenschutz-Grundverordnung 2016/679, „ DS-GVO“ - die ab dem 25. Mai 2018 gelten wird) eine Übermittlung, wenn der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter „angemessene Garantien" vorgesehen hat.

Diese Garantien können weiterhin durch die bekannten Instrumentarien gewährleistet werden.

Mitteilung der EU-Kommission

Datenschutzkonferenz veröffentlicht Kurzpapiere zum neuen Datenschutzrecht

Die Übergangszeit von zwei Jahren seit Inkrafttreten der DS-GVO bis zum Wirksamwerden nutzen die Aufsichtsbehörden, um Interessierten und Verantwortlichen die neuen Rechtsgrundlagen und deren Anforderungen näher zu bringen. Dazu haben einige Aufsichtsbehörden eigene Rubriken auf ihren Internetseiten gestartet. Bei der Umsetzung der Verordnung ist eine abgestimmte und einheitliche Sichtweise unabdingbar.

Als Ergebnis einer gemeinsamen Arbeit veröffentlicht die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) seit geraumer Zeit gemeinsame Kurzpapiere zur DS-GVO:

https://www.bfdi.bund.de/DE/Home/Kurzmeldungen/DSGVO_Kurzpapiere1-3.html

Diese sollen als erste Orientierung dienen, wie nach Auffassung der Datenschutzkonferenz die Datenschutz-Grundverordnung im praktischen Vollzug angewendet werden sollte. Dabei wird betont, dass diese Auffassung unter dem Vorbehalt einer zukünftigen — möglicherweise abweichenden — Auslegung durch den Europäischen Datenschutzausschuss stehe.
Im Kurzpapier Nr. 15 behandelt die Datenschutzkonferenz nun das Thema „ Videoüberwachung“:

Videoüberwachung Download Kurzpapier - Videoüberwachung nach der Datenschutz-Grundverordnung (PDF, 322KB)

Heimliche Aufnahme per Smartphone rechtfertigt außerordentliche Kündigung

Ein Arbeitnehmer, der zu einem Personalgespräch eingeladen war und dieses heimlich mit seinem Smartphone aufgenommen hatte, darf fristlos gekündigt werden. Das entschied das Hessische Landesarbeitsgericht (LAG) in einem Urteil vom 23.08.2017 (Aktenzeichen: 6 Sa 137/17).

Das LAG Hessen stellt in seinem Urteil fest:
„Der heimliche Mitschnitt eines Personalgesprächs ist grundsätzlich geeignet, sowohl eine ordentliche verhaltensbedingte als auch eine außerordentliche Kündigung ‚an sich' zu rechtfertigen. Dabei kommt es nicht entscheidend auf die strafrechtliche Würdigung an. Maßgebend ist die mit diesem Verhalten verbundene Verletzung der dem Arbeitnehmer nach § 241 Abs. 2 BGB obliegenden Pflicht zur Rücksichtnahme auf die berechtigten Interessen des Arbeitgebers.

Das heimliche Mitschneiden des Gesprächs durch den Arbeitnehmer ist rechtswidrig, weil aus dem allgemeinen Persönlichkeitsrecht auch das durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 2 GG gewährleistete Recht auf die Wahrung der Unbefangenheit des gesprochenen Wortes folgt. Das Grundrecht aus Art. 2 Abs. 1 GG schützt auch Rechtspositionen, die für die Entfaltung der Persönlichkeit notwendig sind. Dazu gehört in bestimmten Grenzen, ebenso wie das Recht am eigenen Bild, das Recht am gesprochenen Wort. Deshalb darf grundsätzlich jedermann selbst und allein bestimmen, wer sein Wort aufnehmen soll sowie ob und von wem seine auf einen Tonträger aufgenommene Stimme wieder abgespielt werden darf. Das Grundrecht umfasst die Befugnis des Menschen, selbst zu bestimmen, ob seine Worte einzig seinem Gesprächspartner, einem bestimmten Kreis oder der Öffentlichkeit zugänglich sein sollen…"

Hessenrecht
Landesrechtsprechungsdatenbank