Datenschutz newsbox

Ausgabe
10
2016

Editorial 2
Geldwäscherichtlinie datenschutzrechtlich bedenklich 2
Fragen und Antworten zum EU-US Privacy Shield 3
EU-Kommission veröffentlicht Leitfaden zum Privacy Shield 3
BITKOM bietet FAQ-Sammlung zur DS-GVO 4
Fortgeltung von Einwilligungen unter der DS-GVO 4
Das berufliche Leitbild der Datenschutzbeauftragten 4
Anforderung an Meldung von Datenpannen 5
Google aktualisiert ADV-Verträge zur Nutzung von Google Analytics 5
Absicherung von Telemediendiensten nach Stand der Technik 5
BSI: 10 Dinge, die Sie bei einer Infektion tun sollten 6
Hinweise zum Datenschutzbeauftragten nach der DS-GVO 6
Top aktuell: Vertiefungsworkshops zur Datenschutz-Grundverordnung 6
Bußgeld wegen unzulässiger Mitgliederwerbung 7
Handbuch Arbeitnehmerdatenschutz 7
Kostenverteilung für Vor-Ort-Kontrollen bei ADV 8
Die Datenschutz-Grundverordnung im Überblick 8
Datenschutzrechtliche Einordnung von externen Mitarbeitern 9
ADV-Vertrag mit freiem Mitarbeiter in Heimarbeit/Telearbeit? 9
EuGH eröffnet Interessenabwägung für Telemedien-dienste-Anbieter bei Speicherung von IPAdressen 10

DATAKONTEXT

Editorial

Datenschutz kann nicht nur ein Schild sein, um Betroffene vor Verletzung ihrer Persönlichkeitsrechte zu bewahren. Datenschutz lässt sich manchmal auch wie ein Schild vor sich herschieben, wenn Menschen möglicherweise begangene Fehler nicht zugeben wollen.

Mit dem Datenschutz in neuen Produkten und Dienstleistungen verhält es sich dabei, wie mit Airbags in Auto. Sinnvoll ist es, Datenschutz schon während des Fertigungsprozesses zu integrieren und nicht nach der Fertigstellung. Das wird meist teuer oder zumindest umständlich.
Die Frage, ob der Datenschutz bei Innovationen nicht als Hemmschuh, sondern als ein Korrektiv begriffen werden muss, stellt sich immer wieder.

Und auch beim Feiern sollte man den Datenschutz nicht vergessen, was nicht heißt, dass Datenschutz und Spaß sich ausschließen!

Selbstverständlich sollte Datenschutz und der Wert von Persönlichkeitsrechten nicht nur Erwachsenen vorbehalten sein, sondern gerade auch Kindern.

Zwar keine neue, aber doch eine Erkenntnis der letzten Tage: Persönlichkeitsrechte sind auch auf Sozialen Medien zu wahren und gehen ggf. der Meinungsfreiheit vor.

Noch eine Binsenweisheit zum Schluss, die natürlich auch für den Datenschutz gilt: Unwissenheit schützt vor Strafe nicht!

Ihr Levent Ferik

Geldwäscherichtlinie datenschutzrechtlich bedenklich

Nach einem von Peter Schaar, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit a.D. Vorsitzender der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID), vorgelegten Kurzgutachten begegnet der von der Europäischen Kommission am 5. Juli 2016 vorgelegte Vorschlag zur Überarbeitung der Vierten EU-Geldwäscherichtlinie (2015/849 v. 20.5.2015 - GW-RL) erheblichen datenschutzrechtlichen Bedenken.
Die im Entwurf vorgesehene ausnahmslose Identifikationspflicht der Nutzer von Online-Bezahlverfahren widerspreche dem in Art. 8 EU-Grundrechtecharta verbürgten Grundrecht auf Datenschutz. Sie verfehle insbesondere die Vorgaben des Europäischen Gerichtshofs zur Vorratsdatenspeicherung (EuGH, 08.04.2014 - C-293/12 und C-594/12).
Zudem bestünden erhebliche Zweifel, inwieweit der vorgeschlagene Wegfall anonymer Bezahlmöglichkeiten im Internet kompatibel sei mit dem durch die Datenschutzgrundverordnung (2016/697 - DS-GVO) und der Datenschutzrichtlinie für Polizei und Justiz (RL 2016/680 - DS-JI-RL) vorgegebenen Rahmen.

Quelle: Prepaid Verband Deutschland e.V.

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

Fragen und Antworten zum EU-US Privacy Shield

Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen hat einen Leitfaden erarbeitet und veröffentlicht, welcher einen Überblick über die Regelungen des EU-US Privacy Shield ermöglichen soll. Der Leitfaden richtet sich schwerpunktmäßig an verantwortliche Stellen.
Zur Umsetzung der Angemessenheitsentscheidung der EU-Kommission über das EU-US Privacy Shield sind Abstimmungen zwischen den Aufsichtsbehörden in Deutschland und der EU erforderlich – auch um gemeinsame Verständnisse in Auslegungsfragen zu erreichen. Nach Angaben der LDI NRW werden Informationen deshalb kontinuierlich aktualisiert, erweitert und gegebenenfalls angepasst.

Der Leitfaden setzt sich mit folgenden Fragen auseinander und versucht diese zu beantworten:

1. An welcher Stelle ist das EU-US Privacy Shield für verantwortliche Stellen relevant?
2. Darf das EU-US Privacy Shield ab sofort herangezogen werden, um ein angemessenes Datenschutzniveau für Datenübermittlungen in die USA zu gewährleisten?
3. Welche Bedenken bestehen auf Seiten der europäischen Datenschutzbehörden und welche Auswirkungen haben sie?
4. Welche Prüfpflichten obliegen verantwortlichen Stellen?
5. Gibt es Übergangsregelungen?
6. Können alle US-Unternehmen an der Selbstzertifizierung teilnehmen?
7. Welche Inhalte haben die Grundsätze des EU-US Privacy Shield?
8. Gibt es Ausnahmen von den Grundsätzen des EU-US Privacy Shield?
9. Welche Betroffenenrechte ergeben sich aus dem EU-US Privacy Shield?
10. Sind besondere Vorgaben hinsichtlich Personaldaten zu beachten?
11. Welche staatlichen Stellen überwachen die Einhaltung des EU-US Privacy Shield?
12. Welche Rolle hat die Ombudsperson des EU-US Privacy Shield inne?
13. Welche Anforderungen sind zu beachten, wenn ein datenempfangendes US-Unternehmen als Auftrags(daten)verarbeiter tätig wird?

Quelle: Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

EU-Kommission veröffentlicht Leitfaden zum Privacy Shield

Die Europäische Kommission hat einen Leitfaden zum Privacy-Shield veröffentlicht. Diesen können Interessierte auch in der deutschen Übersetzung abrufen.
Der Leitfaden gibt nicht nur Antworten auf die Frage "Was ist der EU-US-Datenschutzschild und warum brauchen wir ihn?", sondern gibt auch eine Erklärung zu der Frage, wie genau denn der Schutzschild überhaupt funktioniert.

Für Betroffene besonders interessant dürften die Ausführungen sein, welche Verpflichtungen, die dem Datenschutzschild angeschlossenen Unternehmen haben und welche Rechte im Zusammenhang mit der Verwendung personenbezogenen Daten der Betroffenen bestehen.

Quelle: Europäische Kommission

BITKOM bietet FAQ-Sammlung zur DS-GVO

Die Datenschutz-Grundverordnung ist kürzlich in Kraft getreten und muss jetzt von den Unternehmen umgesetzt werden. Stichtag für die Anwendung sämtlicher Regelungen in den Mitgliedsstaaten der EU ist der 25. Mai 2018. Bis dahin muss auch die nationale Gesetzgebung angepasst und Details der Verordnung von den Datenschutzbehörden konkretisiert werden.
Unter dem Titel "Was muss ich wissen zur EU-Datenschutz Grundverordnung?" bietet die BITKOM eine umfangreiche Sammlung häufig gestellter Fragen, die sich vielen Betrieben im Rahmen der Umsetzung der DS-GVO stellen werden.
Der BITKOM bietet die FAQ-Sammlung mit dem Ziel an, den Einstieg in die Planung zur Umsetzung der DS-GVO zu erleichtern und Unternehmen auf die wesentlichen Veränderungen und teilweise Neuerungen aufmerksam zu machen. Die Sammlung soll gerade kleinen und mittleren Unternehmen eine Checkliste an die Hand geben, um möglichst zielgerichtet innerhalb des Unternehmens die richtigen Prozesse in Gang zu setzen. Die aktuelle Publikation zeigt damit, welche Änderungen außerdem konkret auf die Unternehmen zukommen.

Quelle: Bitkom (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.)

Fortgeltung von Einwilligungen unter der DS-GVO

Der Düsseldorfer Kreis stellt in seinem Beschluss vom 13./14. September 2016 klar, nach welchen Kriterien bisher erteilte Einwilligungen unter der Datenschutz-Grundverordnung fortgelten.
Danach gelten bisher erteilte Einwilligungen fort, sofern sie der Art nach den Bedingungen der Datenschutz-Grundverordnung entsprechen (Erwägungsgrund 171, Satz 3 Datenschutz-Grundverordnung). Bisher rechtswirksame Einwilligungen erfüllen grundsätzlich diese Bedingungen, so die Meinung des Düsseldorfer Kreises. Informationspflichten nach Artikel 13 Datenschutz-Grundverordnung müssten dafür nicht erfüllt sein, da sie keine Bedingungen im Sinne des genannten Erwägungsgrundes seien.
Der Beschluss nennt aber auch Bedingungen der DS-GVO deren Nichterfüllung zur Unwirksamkeit von bereits erteilten Einwilligungen führen:

- Freiwilligkeit („Kopplungsverbot“, Artikel 7 Absatz 4 in Verbindung mit Erwägungsgrund 43 Datenschutz-Grundverordnung),
- Altersgrenze: 16 Jahre (soweit im nationalen Recht nichts anderes bestimmt wird; Schutz des Kindeswohls, Artikel 8 Absatz 1 in Verbindung mit Erwägungsgrund 38 Datenschutz-Grundverordnung)

Quelle: Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

Das berufliche Leitbild der Datenschutzbeauftragten

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. hat bereits 2004 damit begonnen, die Anforderungen an die Tätigkeit und das Know-how des Datenschutzbeauftragten zu beschreiben. 2009 entstand daraus das erste „Berufliche Leitbild der Datenschutzbeauftragten“ in Europa, auf das sich Mitglieder schriftlich verpflichten müssen, um durch den BvD als entsprechend qualifiziert ausgezeichnet zu werden.
Durch diesen Prozess und die Auszeichnung „Selbstverpflichtung auf das berufliche Leitbild des Datenschutzbeauftragten“ können Unternehmen und Institutionen nachweisen, dass qualifizierte Datenschutzbeauftragte benannt wurden.
Der BvD greift in der vorliegenden dritten Auflage des Leitbilds die Änderungen durch die DSGVO auf und stellt die neuen Aufgaben und Anforderungen ins Verhältnis zur erforderlichen Qualifikation der Datenschutzbeauftragten. Gleichzeitig wurde die vorliegende Ausgabe um eine Detaillierungsebene gekürzt, um die Lesbarkeit zu verbessern.

Quelle: Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Anforderung an Meldung von Datenpannen

Der Grundsatz der Transparenz in der Datenverarbeitung ist gleichermaßen Folge und zwingende Voraussetzung des Rechts auf informationelle Selbstbestimmung. Der Begriff der „Selbst-Bestimmung" besitzt insofern mehrere Schattierungen. Er rekurriert einerseits auf ein Entscheidungs- und Interventionsrecht des Betroffenen. Andererseits meint er aber auch eine Bestandsaufnahme und Verortung im Hinblick auf die eigenen Daten.
Die Informationspflicht bei unrechtmäßiger Kenntnisnahme durch Dritte nimmt eine Sonderstellung unter den Betroffenenrechten ein. Die datenverarbeitenden Stellen sind bei Pannen nicht nur verpflichtet, den Informationsabfluss gegenüber Betroffenen und Aufsichtsbehörden offenzulegen, sie müssen auch geeignete Hilfestellungen zur Verhinderung schwerwiegender Folgen anbieten.
Wenn sensible Daten im Unternehmen abhandenkommen, drohen meist schwer zu kalkulierende Auswirkungen – vom Vertrauensverlust bei Kunden, Image-Schäden gegenüber Geschäftspartnern bis hin zu großen finanziellen Einbußen, die sich auf das Jahresergebnis niederschlagen können. Welche neuen Anforderungen an die Meldung von Datenpannen in der Grundverordnung verankert sind, hat das BayLDA in einem neuen kurzen Papier zusammengefasst. Das Dokument kann nachfolgend heruntergeladen werden.

Quelle: Bayerisches Landesamt für Datenschutzaufsicht

Google aktualisiert ADV-Verträge zur Nutzung von Google Analytics

Nach dem der HmbBfDI bereits Juni 2016 darauf hingewiesen hatte, dass die Angemessenheit des Datenschutzniveaus, was die Nutzung von Google Analytics angeht, nach der Safe Harbor-Entscheidung des EuGH (06.10.2016) nicht mehr auf das Safe Harbor-Abkommens gestützt werden kann, war es eine Frage der Zeit, wann Google dieses Defizit durch das nunmehr mögliche Instrument des Privacy Shields beheben wird.

Google informiert auf seinem Blog, dass Google bzgl. der Übermittlung von personenbezogenen Daten in die USA neuerdings auf die Selbstzertifizierung nach dem Privacy Shield verweisen kann. Wie auf dem Blog von Herrn Dr. Piltz zusammengefasst, hat Google nach erfolgter Zertifizierung auch seinen alten Vertrag zur Auftragsdatenverarbeitung angepasst und stellt diesen seinen deutschen Kunden zur Verfügung.
Der bislang unter Ziffer 4.7 geführte Verweis auf Safe Harbor ist nun getilgt, so dass anzunehmen ist, dass Google in den neuen Verträgen auf den Privacy Shield Bezug nehmen wird.

Absicherung von Telemediendiensten nach Stand der Technik

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat eine Cyber-Sicherheitsempfehlung zur Absicherung von Telemediendiensten nach Stand der Technik veröffentlicht, die unter Beteiligung des Bitkom e. V. und des Expertenkreises Internetbetreiber der Allianz für Cyber-Sicherheit entstanden ist. Das Papier schlägt Maßnahmen vor, wie Telemediendienste gegen unerlaubten Zugriff auf technische Einrichtungen, Verletzung des Schutzes personenbezogener Daten sowie Störungen abgesichert werden können.
Bei den vorgeschlagenen Maßnahmen wird jeweils der Stand der Technik berücksichtigt, d. h., dass die Maßnahmen auf den Erfahrungen und der Expertise des BSI sowie den Vertretern der Internetbranche zu fortschrittlichen Verfahren und Techniken zur Absicherung von Telemediendiensten basieren.
Die Cyber-Sicherheitsempfehlung richtet sich vornehmlich an Anbieter und Verantwortliche von geschäftsmäßig angebotenen Telemediendiensten, beispielsweise Betreiber von Online-Shops und Unternehmen, die Hosting- und Server-Dienstleistungen anbieten.

Quelle: Bundesamt für Sicherheit in der Informationstechnik

BSI: 10 Dinge, die Sie bei einer Infektion tun sollten

Die Beseitigung von Schadprogrammen ist immer eine heikle Sache. Es gibt inzwischen mehr bösartige als gutartige Programme. Die Hersteller von Viren-Schutzprogrammen haben es daher nicht leicht, alle Bedrohungen zu erkennen und dann auch im Falle eines Falles zu entfernen. Aktuelle Schadprogramme werden in den ersten Stunden/Tagen nicht gefunden. Kein Fund des Viren-Schutzprogrammes bedeutet somit nicht, dass der Rechner nicht doch infiziert ist
Wenn Sie Ihren Rechner beispielsweise geschäftlich oder für Bankgeschäfte nutzen, müssen Sie auch nach einer beseitigten Infektion sehr vorsichtig sein, da nie hundertprozentig sicher ist, dass das Schadprogramm vollständig entfernt wurde.
Häufig verändern Schadprogramme auch sicherheitsrelevante Einstellungen des Betriebssystems, die nicht immer einfach rückgängig gemacht werden können.
Das Bundesamt für Sicherheit in der Informationstechnik informiert auf seiner Seite "BSI für Bürger" welche Schritte in einem solchen Fall einzuleiten sind und welche besser nicht.

Quelle: Bundesamt für Sicherheit in der Informationstechnik

Hinweise zum Datenschutzbeauftragten nach der DS-GVO

In einem offenen Brief an die Artikel-29-Datenschutzgruppe gibt CEDPO (The Confederation of European Data Protection Organisations) Anregungen zu Bestellung, Stellung, Aufgaben und Fachkunde des Datenschutzbeauftragten nach der DSGVO.
Um frühzeitig auf die Implementierung der DSGVO vorzubereiten, hat die Artikel-29-Gruppe am 26. Juli 2016 ein sog. "Fablab" veranstaltet, das in Form eines Workshops die Brücke zwischen gesetzlichen Konzeptionen und der operativen Durchführung schlagen möchte. CEDPO wurde zu diesem Treffen in Brüssel eingeladen, um auf Fragestellungen zum Datenschutzbeauftragten einzugehen. Eine Zusammenfassung der Ergebnisse des Workshops findet sich hier.
Im Nachgang zum Workshop hat CEDPO erste Antworten auf die aufgeworfenen Fragen formuliert und in einem offenen Brief an die Artikel-29-Gruppe versendet. Hierbei wurde u.a. auf die geforderte Fachkunde sowie die Möglichkeiten einer externen oder internen Bestellung ebenso eingegangen, wie das Vorliegen möglicher Interessenkonflikte, die Haftung sowie der Umfang seiner/ihrer gesetzlich zugewiesenen Aufgaben.

Der Brief kann hier abgerufen werden.

Top aktuell: Vertiefungsworkshops zur Datenschutz-Grundverordnung


VERTIEFUNGSWORKSHOPS ZUR DATENSCHUTZ-GRUNDVERORDNUNG

ZIEL DER WORKSHOP-REIHE

HINWEIS

Weitere Vertiefungsworkshops zu den Themen Beschäftigtendatenschutz, Praxis der Transparenzpflichten, Datenschutz-Folgenabschätzung usw. sind in der Planung.

REFERENTEN

Paul Gürtler,

Bettina Rohrecht, LL.M.,

RA Dr. Jens Eckhardt,

Dr. Niels Lepperhoff,

RA Thomas Mühlein,

Steffen Weiß, LL.M.,

Für die betroffenen Unternehmen heißt es „der Countdown läuft“, um bis Mai 2018 die Organisation, Prozesse und Verarbeitungen an die neuen Regelungen der Datenschutz-Grundverordnung (DS-GVO) anzupassen. Hier bieten Ihnen unsere Vertiefungsworkshops die Möglichkeit, Spezialthemen zu erarbeiten und sich und Ihr Unternehmen fit für den Übergang vom BDSG zur DS-GVO zu machen.

Die folgenden Themen haben wir für Sie bereits als Vertiefungsworkshop aufbereitet:

Vertiefungsworkshop 1: Der Umsetzungsplan vom BDSG zur DS-GVO
am 28.11.2016 in Köln
Vertiefungsworkshop 2: Dokumentation, Meldepflichten und IT-Sicherheitsmanagement nach der DS-GVO
am 06.12.2016 in Köln
Vertiefungsworkshop 3: Auftragsverarbeitung nach DS-GVO - Grundlagen für den Übergang vom BDSG zur DS-GVO
am 07.12.2016 Köln

Sie erhalten konkrete Vorschläge und Umsetzungstipps, wie die neuen Anforderungen in der kurzen Übergangszeit realisiert werden können. Leitfäden, Checklisten und Musterverträge helfen Ihnen, den Änderungsprozess erfolgreich zu gestalten. Für ausführliche Informationen klicken Sie bitte oben auf den jeweiligen Workshop.

Bußgeld wegen unzulässiger Mitgliederwerbung

Das Sozialgericht Düsseldorf hat eine Betriebskrankenkasse zur Zahlung einer Vertragsstrafe in Höhe von 45.000 € an die AOK Rheinland/Hamburg verurteilt.
Die klagende AOK und die beklagte BKK stehen im Wettbewerb zueinander. Die Klägerin schloss Dezember 2014 mit der Beklagten einen Unterlassungsvergleich. Danach hat es die Beklagte unter Androhung einer Vertragsstrafe u.a. zu unterlassen, bei potentiellen Kunden ohne Einwilligung in die Telefonie für Werbezwecke anzurufen und mit Wechselprämien oder Geldbeträgen zu werben, ohne ausführlich über die jeweiligen Voraussetzungen der Satzung für den Erhalt dieser Geldbeträge aufzuklären.
In der Folgezeit kontaktierte ein von der Beklagten beauftragtes Unternehmen mehrere Versicherte der Klägerin, um diese abzuwerben. Darin sah die Klägerin einen Verstoß gegen die Unterlassungsvereinbarung und forderte in drei Fällen jeweils 15.000 € Vertragsstrafe. Es habe keine ausdrückliche Einwilligung in die Telefonwerbung vorgelegen und die Beklagte habe zudem unzureichend über die Voraussetzungen ihres Bonusprogramms informiert.

Die 27. Kammer des Sozialgerichts Düsseldorf folgte der Argumentation der Klägerin. Die Beklagte habe keine wirksame Einwilligung der kontaktierten Personen in die Telefonwerbung dargelegt. Eine Registrierung bei einer Online-Gewinnspielseite stelle – entgegen der Auffassung der Beklagten – keine ausdrückliche Einwilligung in eine Telefonwerbung zum Zwecke der Mitgliederwerbung dar. Dies gelte auch dann, wenn im Rahmen des Gewinnspiels Fragen zur Krankenversicherung gestellt würden und die Option "hohe Bonuszahlungen – mehr Infos bitte – wählbar sei. Darüber hinaus habe die Beklagte die kontaktierten Personen auch nicht ausreichend und nachhaltig über die satzungsmäßigen Voraussetzungen der Bonuszahlungen informiert. Sie habe dabei insbesondere den Eindruck erweckt, über die Teilnahme am Bonusprogramm seien die gesamten Kosten der angebotenen privaten Zusatzversicherungen zu erwirtschaften.

Urteil vom 08.09.2016 - S 27 KR 629/16 - nicht rechtskräftig -

Quelle: Justizministerium Nordrhein-Westfalen

Kostenverteilung für Vor-Ort-Kontrollen bei ADV

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

Frage des GDD-Erfa-Kreises Würzburg:
Es ist gesetzlich nicht zwingend erforderlich, Vor-Ort Kontrollen im Rahmen der Auftragsdatenverarbeitung durchzuführen. Es ist auch die Vorlage von Zertifikaten möglich. Sollten diese allerdings nicht aussagekräftig sein oder es zu vermehrten Datenschutzvorkommnissen beim Dienstleister kommen, so ist es angebracht, die technischen und organisatorischen Maßnahmen im Rahmen einer Vor-Ort Überprüfung zu kontrollieren.
Frage:
Darf der Dienstleister hierzu den Aufwand, der für ihn durch die Vor-Ort-Prüfung durch das Zur-Verfügungstellen von Personal entsteht, dem Auftraggeber in Rechnung stellen (auch wenn dies vertraglich nicht explizit geregelt wurde)?

Antwort BayLDA:
Hierzu können wir nichts sagen. Das ist keine datenschutzrechtliche, sondern eine zivilrechtliche Streitfrage zur Auslegung eines Vertrags für nicht konkret geregelte Sachverhalte (Kernfrage: Was ist dem Auftragnehmer an Aufwand entschädigungslos zumutbar, damit der Auftraggeber seine BDSG-Kontrollpflichten erfüllen kann, und ab wann besteht ein unzumutbarer Aufwand, für den der Auftragnehmer einen angemessenen Aufwand-Ersatz verlangen kann?). Am besten ist natürlich eine Festlegung im Vertrag dazu.

Datenschutzrechtliche Einordnung von externen Mitarbeitern

Frage des GDD-Erfa-Kreises Würzburg:
a) Unternehmen (A) beauftragt einen Dienstleister (B), bei A im Haus regelmäßige Dienste (mit personenbezogenen Daten) auszuführen / zu bearbeiten. B schickt hierfür eigene Angestellte, die bei A im Unternehmen mitarbeiten und gefühlt in das Unternehmen A miteingegliedert sind.

b) Unternehmen (A) beauftragt einen Dienstleister (B), bei A im Haus regelmäßige Dienste (mit personenbezogenen Daten) auszuführen / zu bearbeiten. B schickt hierfür freie/selbständige Mitarbeiter (gerade keine Angestellten, selbständige Mitarbeiter haben „nur" ein Vertragsverhältnis mit B), die bei A im Unternehmen mitarbeiten und gefühlt in das Unternehmen A miteingegliedert sind.

c) Wie bei a) und b), nur beschränkt sich die Dienstleistung auf Information und Beratung; eine Datenverarbeitung im Unternehmen durch die Mitarbeiter des B findet nicht statt.

Frage:
Ist jeweils bei a), b) und c) ein ADV-Vertrag notwendig und wenn ja, wer mit wem? Falls ein ADV-Vertrag notwendig ist, wessen technischen und organisatorischen Maßnahmen sind im ADV-Vertrag aufzulisten?

Antwort BayLDA:
Wenn die von extern kommenden Personen „wie Mitarbeiter" miteingegliedert sind und unter Aufsicht und nach Anweisung des Unternehmens A tätig werden, halten wir die Annahme eines ADV-Verhältnisses zu B bzw. zu den extern Beschäftigten oder freien Mitarbeitern nicht für sachgerecht. Diese Personen sind als „sonstige Beschäftigte" (vergleichbar den arbeitnehmerähnlichen Personen nach § 3 Abs. 11 Nr. 6 BDSG) auf das Datengeheimnis nach § 5 BDSG zu verpflichten und wie die eigenen Mitarbeiter von der Unternehmensleitung A im Hinblick auf deren datenschutzrechtlichen Verantwortlichkeit zu beaufsichtigen.

ADV-Vertrag mit freiem Mitarbeiter in Heimarbeit/Telearbeit?

Frage des GDD-Erfa-Kreises Würzburg:
Unternehmen (A) hat einen freien Mitarbeiter (F). Dieser ist im Unternehmen von A praktisch wie ein Arbeitnehmer tätig. Dieser ist bei sich zuhause tätig und bekommt die Daten zum Bearbeiten per Post/VPN-Zugriff oder erhebt sie selbst.
Ist ein ADV-Vertrag zu schließen oder reicht die Verpflichtung nach § 5 BDSG? Wenn ein ADV-Vertrag notwendig ist, wessen technischen und organisatorischen Maßnahmen sind dann aufzulisten?

Antwort BayLDA:
Wie auch bei der letzten Frage halten wir die Annahme eines ADV-Verhältnisses zu solchen wie Arbeitnehmer unter Weisung und Aufsicht des Unternehmens A tätigen freien Mitarbeitern (im Unternehmen oder in Heimarbeit) nicht für sachgerecht.
Diese Personen sind als arbeitnehmerähnliche Personen nach § 3 Abs. 11 Nr. 6 BDSG auf da Datengeheimnis nach § 5 BDSG zu verpflichten (siehe so auch unser Info-Blatt zur Verpflichtung unter https://www.lda.bayern.de/media/info_datengeheimnis.pdf und wie die eigenen Mitarbeiter von der Unternehmensleitung A im Hinblick auf deren datenschutzrechtlichen Verantwortlichkeit zu beaufsichtigen.

EuGH eröffnet Interessenabwägung für Telemediendienste-Anbieter bei Speicherung von IP-Adressen

Mit seinem Urteil (Rechtssache C-582/14) vom 19.10.2016 hat der EuGH zunächst festgestellt, dass die dynamische Internetprotokoll-Adresse eines Nutzers für den Betreiber der Website ein personenbezogenes Datum darstellt, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, den betreffenden Nutzer anhand der Zusatzinformationen, über die dessen Internetzugangsanbieter verfügt, bestimmen zu lassen.
Der Gerichtshof führt hierzu aus, dass es in Deutschland offenbar rechtliche Möglichkeiten gibt, die es dem Anbieter von Online-Mediendiensten erlauben, sich insbesondere im Fall von Cyberattacken an die zuständige Behörde zu wenden, um die fraglichen Informationen vom Internetzugangsanbieter zu erlangen und anschließend die Strafverfolgung einzuleiten.
Zudem könne der Betreiber einer Website ein berechtigtes Interesse daran haben, bestimmte personenbezogene Daten der Nutzer zu speichern, um sich gegen Cyberattacken zu verteidigen.
Der EuGH stellt ebenso fest, dass das Unionsrecht einer Regelung eines Mitgliedstaats entgegensteht, nach der ein Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung nur erheben und verwenden darf, soweit ihre Erhebung und ihre Verwendung erforderlich sind, um die konkrete Inanspruchnahme der Dienste durch den betreffenden Nutzer zu ermöglichen und abzurechnen, ohne dass der Zweck, die generelle Funktionsfähigkeit der Dienste zu gewährleisten, die Verwendung der Daten über das Ende eines Nutzungsvorgangs hinaus rechtfertigen kann.
Die Verarbeitung personenbezogener Daten ist nach dem Unionsrecht u. a. rechtmäßig, wenn sie zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, erforderlich ist, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.
Die deutsche Regelung schränke nach ihrer in der Lehre überwiegend vertretenen Auslegung die Tragweite dieses Grundsatzes ein, indem sie es ausschließt, dass der Zweck, die generelle Funktionsfähigkeit des Online-Mediums zu gewährleisten, Gegenstand einer Abwägung mit dem Interesse oder den Grundrechten und Grundfreiheiten der Nutzer sein kann.

Gerichtshof der Europäischen Union