Datenschutz newsbox

Ausgabe 7 2019

Editorial: 2

Zulässigkeit der Datenverarbeitung für Akkreditierung 3

Übermittlungen nach U.S. CLOUD Act nicht ohne internationales Abkommen 3

ULD aktualisiert Praxis-Reihe 4

Datenschutzrechtliche Anforderungen und Entwicklungen von Löschkonzepten (Anzeige) 4

Stellungnahme zur Evaluation der DS-GVO 5

Nutzung von Office365 in Schulen kritisch 5

DSK veröffentlicht Beschluss zum Thema „Asset-Deal“ 6

Einführung in den Datenschutz (Anzeige) 6

Best Practice bei Auskunftsverlangen 6

Grenze der Bestellpflicht für Datenschutzbeauftragte angehoben 7

BSI-Empfehlung für sichere Konfiguration von MS-Office-Produkten 7

Hinweispflichten bei Auskunftsbegehren 8

Datenschutzkonforme E-Mail-Weiterleitung bei Abwesenheit oder Ausscheiden aus dem Betrieb 8

BvD gründet Dachverband für Datenschutzbeauftragte 9

Jetzt neu: Handbuch Beschäftigtendatenschutz (Anzeige) ... 9

Beschwerde gegen personalisierte Online-Werbung 10

Maximale Datensparsamkeit bei Online-Terminen und Umfragen 10

DATAKONTEXT

Editorial:

Die Landesbeauftragte für den Datenschutz (LfD) Niedersachsen, Barbara Thiel, hat im November 2018 in 150 Städten, Landkreisen und Gemeinden eine Abfrage zum Sachstand der Umsetzung der seit dem 25. Mai 2018 unmittelbar geltenden DS-GVO durchführen lassen. Die Ergebnisse zeigen, dass es auch bei den Kommunen noch mit der Umsetzung hapert.

Nachsitzen müssen die Kommunen insbesondere, weil sie noch Nachholbedarf bei der Durchführung von Datenschutz-Folgenabschätzungen und der Meldung sogenannter Datenpannen haben. Einen „Prima-Stempel" vergab die LfD dagegen für alle Kommunen, was die Pflicht zur Bestellung eines Datenschutzbeauftragten angeht. Hier gab es keine Kommune, die bei dieser Aufgabe gepatzt hat.
Frei nach dem Motto „Unter den Blinden ist der Einäugige König" lässt es sich wohl tatsächlich als positiv bewerten, dass fast alle angeschriebenen Städte, Landkreise und Gemeinden inzwischen mit der Überprüfung ihrer Verträge zur Auftragsverarbeitung begonnen haben.

Dabei unterscheiden sich die von den Kommunen als Grund für ihre Umsetzungsschwierigkeiten genannten Angaben nicht wesentlich von den Gründen, die die Vertreter der Privatwirtschaft oftmals angeben: Mangelnde zeitliche und personelle Ressourcen, Probleme bei der Zusammenführung von Informationen aus den einzelnen Fachämtern sowie das Fehlen verbindlicher Muster und Vorgaben. Zumindest der letzte Grund hört sich aber ein wenig nach „Ich habe meine Hausaufgaben nicht, weil der Hund diese aufgefressen hat" an. Orientierungshilfen und Mustertexte gibt es mittlerweile zuhauf. Diese nehmen den Verantwortlichen aber nicht die Arbeit ab.

Das Ergebnis einer repräsentativen Befragung unter mehr als 500 Unternehmen aus Deutschland, die der Digitalverband Bitkom letztes Jahr im Rahmen seiner Privacy Conference vorgestellt hat, zeigte, dass auch der deutschen Privatwirtschaft nach Fristablauf für die Umsetzung der DS-GVO ein ähnliches Zeugnis ausgestellt werden muss.
Erst ein Viertel (24 Prozent) der Unternehmen in Deutschland gab im September 2018 an, die DS-GVO vollständig umgesetzt zu haben. Weitere 40 Prozent hatten zu diesem Zeitpunkt die Regeln größtenteils umgesetzt, drei von zehn (30 Prozent) teilweise. Gerade erst begonnen mit den Anpassungen hatten damals fünf Prozent der Unternehmen.
Auch wenn das Klassenziel und die Versetzung nicht gefährdet sind, muss in Sachen Umsetzung der DS-GVO noch ein wenig nachgearbeitet werden, 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

Zulässigkeit der Datenverarbeitung für Akkreditierung

Frage des GDD-Erfa-Kreises Coburg:
Veranstalter erheben zum Schutz der Besucher/öffentliche Sicherheit von dem auf der Veranstaltung arbeitenden Personal zur Akkreditierung den Vor- und Nachnamen sowie die Privatanschrift und das Geburtsdatum. Am Veranstaltungstag werden diese Daten abgeglichen, indem der Mitarbeiter seinen Personalausweis vorzeigt. Dass an der Veranstaltung eingeteilte Personal gibt entweder die Daten direkt in die vorgesehene Online-Maske des Veranstalters ein und willigt ein, dass die Daten für den Zweck verarbeitet werden. Auch die Infopflichten, gem. Art. 13 DS-GVO, werden bereitgestellt, wobei betont wird, dass zwar eine Online-Maske vom Veranstalter zur Verfügung gestellt wird, verantwortliche Stelle aber der jeweilige Arbeitgeber ist, oder aber der jeweilige Arbeitgeber gibt diese Daten an den Veranstalter weiter. Im Arbeitsvertrag ist hierzu nichts geregelt. Am Veranstaltungstag selbst erfolgt dann bei der Eingangskontrolle der Datenabgleich mit den davor erhobenen Daten und dem Personalausweis, der vorgezeigt wird.
Dürfen die Privatanschrift sowie das Geburtsdatum des arbeitenden Personals für die Akkreditierung erhoben werden?

Antwort des BayLDA:
Nach unserer Ansicht kommen als Rechtsgrundlage Art. 6 lit. a) DS-GVO der Mitarbeiter sowie Art. 6 lit. f) DS-GVO in Betracht.
Da es möglicherweise Mitarbeiter gibt, die mit der Erhebung ihrer Daten nicht einverstanden sind und dann die Freiwilligkeit fraglich ist, würden wir uns daher auf die Datenverarbeitung aufgrund der Interessenabwägung konzentrieren. Entscheidend ist nach unserer Ansicht, ob diese Daten wirklich zur Akkreditierung notwendig sind. Wenn dem so ist, geht unseres Erachtens die Abwägung zugunsten der öffentlichen Sicherheit aus.

Ergänzung der Frage:
Im vorliegenden Fall wurde zwischenzeitlich die Privatanschrift seitens des Veranstalters entfernt und es wird nur noch das Geburtsdatum erhoben, da dies für die Akkreditierung notwendig sei. Das arbeitende Personal stellt sich jedoch auf den Standpunkt, dass eine eindeutige Identifizierung auch anhand des sowieso zu tragenden Lichtbildausweises möglich ist.

Antwort des BayLDA:
Die Erhebung des Geburtsdatums ist zur eindeutigen Identifizierung sachgerecht und auch ausreichend im Sinne der Erforderlichkeitsprüfung nach Art. 6 Abs. 1 Satz 1 lit. f) DS-GVO; die Privatanschrift muss dazu nicht erhoben werden.

Übermittlungen nach U.S. CLOUD Act nicht ohne internationales Abkommen

In einem Schreiben an den LIBE-Ausschuss des Europäischen Parlaments (EP) macht der Europäische Datenschutzausschuss (EDSA) deutlich, dass für eine rechtmäßige Übermittlung von Daten, die nach dem U.S. CLOUD Act ersucht werden, grundsätzlich ein datenschutzkonformes internationales Abkommen erforderlich ist.
Zudem verständigte sich der EDSA auf Leitlinien zur Videoüberwachung. Diese behandeln sowohl klassische Themen der Videoüberwachung, wie zum Beispiel die Standortwahl oder die Speicherdauer von Aufnahmen, als auch Fragen zu neuen Themenbereichen wie der biometrischen Videoüberwachung.
So stellt der EDSA beispielsweise klar, dass biometrische Daten, die eine dauerhafte Identifizierung von Personen ermöglichen, zu den besonders schützenswerten Daten zählen und daher nur unter sehr strengen Voraussetzungen verarbeitet werden dürfen. Das Tracking von Personen mittels dauerhafter biometrischer Identifizierung, beispielsweise um das Bewegungs- und Kaufverhalten einer Person in einem Kaufhaus nachzuverfolgen, ist dementsprechend grundsätzlich nur mit expliziter Einwilligung der Betroffenen zulässig.

Quelle: Bundesbeauftragter für den Datenschutz und die Informationsfreiheit

ULD aktualisiert Praxis-Reihe

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hat seine Praxisreihe aktualisiert und auf den Stand Juni 2019 gebracht. Aus der Praxisreihe „Datenschutzbestimmungen praktisch umsetzen“ sind folgende Praxisratgeber kostenlos erhältlich:

Datenschutz im Verein: Das Praxisheft soll eine Übersicht darüber geben, welche Datenschutzregeln von Vereinen und Verbänden einzuhalten sind und was im Einzelnen veranlasst werden sollte.

Datenschutzbeauftragte:
Das Praxisheft soll eine Übersicht darüber geben, welche Datenschutzregeln im Zusammenhang mit der Benennung von Datenschutzbeauftragten einzuhalten sind und was im Einzelnen veranlasst werden sollte.

Mustervereinbarung für einen Vertrag zur Auftragsverarbeitung: Das Praxisheft soll eine Übersicht darüber geben, welche Inhalte bei der Abfassung eines Vertrags zur Auftragsverarbeitung von Bedeutung sein können. Die Mustervereinbarung dient dabei als Orientierungshilfe und berücksichtigt die Rechtslage ab dem 25.05.2018.

Informationspflichten: Das Praxisheft soll eine Übersicht darüber geben, welche Datenschutzregeln im Zusammenhang mit der Erfüllung von Informationspflichten einzuhalten sind und was im Einzelnen veranlasst werden sollte.

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.

Fotos und Webcams: Die Broschüre gibt Auskunft über die wichtigsten Fragen zum Datenschutz bei der Erstellung von Bildaufnahmen nach der Datenschutzgrundverordnung der EU (DS-GVO), die Veröffentlichung derartiger Fotografien sowie die Verbreitung der Aufnahmen. Außerdem wird erläutert, unter welchen Voraussetzungen der Betrieb einer Webcam aus datenschutzrechtlicher Sicht zulässig ist. Nicht enthalten sind Fragen der Datenverarbeitung im Bereich des Journalismus und die Fotografie von Einzelpersonen, mit denen ein Vertrag geschlossen wurde.

Quelle: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Stellungnahme zur Evaluation der DS-GVO

Ein Jahr nach dem Inkrafttreten der DS-GVO hat der LfDI zusammen mit der IHK Stuttgart eine erste Bilanz zur Umstellung und Anwendung des neuen Datenschutzrechts gezogen.
Die Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) hat zur Evaluierung der Datenschutz-Grundverordnung (DS-GVO) durch den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Dr. Stefan Brink, wie folgt Stellung genommen:
Das Ziel der DS-GVO war die Vollharmonisierung der Regelungen bei der Verarbeitung personenbezogener Daten in allen Mitgliedstaaten der Europäischen Union (EU). Diese Zielvorgabe konnte jedoch mit der DS-GVO nicht vollumfänglich erreicht werden. Zwar stellt die Grundverordnung unmittelbar anwendbares Datenschutzrecht dar, gleichwohl sind die Mitgliedstaaten an vielen Stellen weiterhin in der Pflicht nationale Regelungen vorzusehen. Dies gilt im Besonderen für die Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt. So gesehen, stellt die DS-GVO eine „hinkende Verordnung“ oder einen Hybrid aus Richtlinie und Verordnung dar. Die umfänglichen Regelungen innerhalb der DS-GVO sind häufig mit dem Wunsch nach Konkretisierung und Spezifizierung verbunden, da der Rechtsanwender regelmäßig mit Unsicherheiten bei der Anwendung des sekundärrechtlichen Datenschutzrechts konfrontiert ist. Auch im Sinne der praktikablen Rechtsanwendung sollten eindeutige und allgemein verständliche Regelungen das Ziel sein, um nicht noch mehr Rechtsunsicherheit bei der Verarbeitung personenbezogener Daten zu erzeugen. Das ist mit Blick auf die Anwendung der DS-GVO im ersten Jahr ihrer Anwendungspflicht nicht gelungen.
Die gesamte Stellungnahme der GDD können Sie unter nachfolgender URL abrufen:

https://www.gdd.de/downloads/stellungnahme-der-gdd-zur-evaluierung-der-ds-gvo

Nutzung von Office365 in Schulen kritisch

In einer aktuellen Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit (HBDI) wird der Einsatz von Microsoft Office 365 in hessischen Schulen als problematisch eingestuft.
Der Hessische Beauftragte für Datenschutz und Informationsfreiheit hatte sich bereits August 2017 zum Einsatz von Office 365 in Schulen geäußert.
Nach der damaligen Bewertung genügte die damalige Ausgestaltung den Anforderungen an eine datenschutzkonforme Nutzung. Ausschlaggebend war schon damals der Einsatz der von Microsoft zur Verfügung gestellten Tools für das Rollen- und Berechtigungskonzepts und die datenschutzkonforme Konfiguration der Protokollierung.
In seiner aktuellen Bewertung muss der Hessische Datenschützer seine Meinung von damals revidieren. Trotz jahrelanger Diskussionen der Aufsichtsbehörden mit Microsoft seien wichtige Fragen noch ungeklärt und Schulen hätten als öffentliche Einrichtungen eine besondere Verantwortung hinsichtlich Zulässigkeit und Nachvollziehbarkeit der Verarbeitung personenbezogener Daten. Des Weiteren müsse insbesondere für solche Stellen die „digitale Souveränität staatlicher Datenverarbeitung gewährleistet sein“. Diese hohen Anforderungen seien aber nicht erfüllt. Bei der Nutzung von Office 365 sei nach wie vor nicht abschließend geklärt, welche Daten wann, wie und warum erhoben und übertragen werden.
Das Problem sei nach Einschätzung des HBDI auch nicht durch die Einholung einer Einwilligung bei den Eltern der betroffenen Schüler zu lösen.

Quelle: Der Hessische Beauftragte für Datenschutz und Informationsfreiheit

DSK veröffentlicht Beschluss zum Thema „Asset-Deal“

Im Nachgang der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder wurde ein Beschluss zum Thema „Asset Deal“ gefasst und einen Katalog von Fallgruppen zusammengestellt.
„Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat sich auf einen Katalog von Fallgruppen verständigt, die im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f i.V.m. Abs. 4 DS-GVO bei einem Asset Deal zu berücksichtigen sind.

Das Papier beschäftigt sich mit folgenden Fallgruppen:

1. Kundendaten bei laufenden Verträgen
2. Bestandskunden ohne laufende Verträge und letzter Vertragsbeziehung älter als drei Jahre
3. Daten von Kundinnen und Kunden bei fortgeschrittener Vertragsanbahnung; Bestandskundinnen und -kunden ohne laufende Verträge und letzter Vertragsbeziehung jünger als 3 Jahre
4. Kundendaten im Falle offener Forderungen
5. Kundendaten besonderer Kategorie nach Art. 9 Abs. 1 DS-GVO

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

Best Practice bei Auskunftsverlangen

Frage des GDD-Erfa-Kreises Coburg:
Die Auskunft nach Art. 15 Abs. 3 DS-GVO regelt, dass der Verantwortliche eine Kopie der zu verarbeitenden Daten zur Verfügung stellt. Muss diese zwingend bei einer Auskunft als Anlage mitgeschickt werden oder reicht es die betreffenden Daten (mit den weiteren Angaben nach Art. 15 Abs. 1 DS-GVO) in dem Antwortschreiben mitzuteilen? Eine Kopie würde nur dann mitgeschickt werden, wenn die betroffene Person explizit danach fragt.

Antwort des BayLDA:
Eine zusätzliche Kopie der Daten muss nicht mitgeschickt werden. Art. 15 Abs. 3 DS-GVO regelt nach unserer Ansicht die bevorzugte Form der Auskunftserteilung und bewirkt keinen zusätzlichen Inhalt für eine Auskunft nach Art. 15 DS-GVO. Es genügt also auch, in einem Antwortschreiben die personenbezogenen Daten der betroffenen Person aufzulisten

Grenze der Bestellpflicht für Datenschutzbeauftragte angehoben

Nach der 2017 beschlossenen Novellierung des Bundesdatenschutzgesetzes (BDSG) hat der Bundestag nun auch das bereichsspezifische Datenschutzrecht des Bundes an die seit Mai 2018 geltende Datenschutz-Grundverordnung (DS-GVO) angepasst.
Mit dem in den frühen Morgenstunden des 28.06.2019 vom Bundestag verabschiedeten zweiten Datenschutzanpassungs- und Umsetzungsgesetz (2. DSAnpUG) werden zahlreiche Gesetze mit den Vorgaben der DS-GVO in Einklang gebracht. Das Gesetz nimmt in 154 Fachgesetzen fast aller Ressorts Änderungen vor. Zu den Regelungsschwerpunkten zählen dabei insbesondere Anpassungen von Begriffsbestimmungen und von Rechtsgrundlagen für die Datenverarbeitung sowie Regelungen zu den Betroffenenrechten. Zudem schafft das verabschiedete Gesetz auch Änderungen im BDSG. Mit dem Argument des Bürokratieabbaus hatte die Unionsfraktionen die Forderung in die Gesetzesberatung eingebracht, die Grenze der Bestellpflicht für einen betrieblichen Datenschutzbeauftragten (§ 38) auf 50 Personen zu erhöhen. Im Rahmen eines Kompromisses haben sich die Koalitionsfraktionen aber schlussendlich doch auf eine Erhöhung von 10 auf 20 Personen, die ständig personenbezogene Daten verarbeiten, verständigt.
Die Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) hat die über ein Jahr andauernde Diskussion rund um das 2. DSAnpUG fortlaufend begleitet und dabei vor allem warnend auf die Entscheidungsträger in den Koalitionsfraktionen eingewirkt, dass eine im Raum stehende Veränderung der Formulierung („Personen, die überwiegend mit der Datenverarbeitung befasst sind“) die Bestellpflicht erheblich aufweichen könnte. Gerade über den kontinuierlich betriebenen Kontakt zu den zuständigen Berichterstattern für Datenschutz konnte die GDD überzeugend darlegen, dass die überlegte Änderung der Formulierung dazu führen würde, dass ein Beschäftigter dann mehr als 50 Prozent seiner Arbeitszeit für die Datenverarbeitung aufwenden müsste, um „überwiegend“ mit der Datenverarbeitung befasst zu sein. Diese Voraussetzung würden nur die wenigsten Mitarbeiter in Unternehmen erfüllen. Die Befreiung von der Bestellpflicht eines Datenschutzbeauftragten im Betrieb führt jedoch nicht zu einem Wegfall anderer datenschutzrechtlicher Pflichten. Am Ende wird mit dem Wegfall eines Datenschutzbeauftragten nicht Bürokratie, sondern Kompetenz und Sachverstand abgebaut. Auch ohne gesetzliche Bestellpflicht sind Unternehmen und Einrichtung gut beraten, einen betrieblichen Datenschutzbeauftragten zu benennen.
Neben technischen Änderungen am BDSG und dem Hinzufügen des § 86 BDSG (Verarbeitung personenbezogener Daten für Zwecke staatlicher Auszeichnungen und Ehrungen) wird auch der für die Praxis so bedeutsame § 26 BDSG an einer Stelle verändert. In § 26 Abs. 2 Satz 3 BDSG entfällt das Schriftformerfordernis für die Einwilligung im Beschäftigtenverhältnis und wird durch die Wörter „hat schriftlich oder elektronisch zu erfolgen“ ersetzt.
Neben dem verabschiedeten Gesetz fordert die Große Koalition die Bundesregierung zudem auf, Art. 85 DS-GVO (Verarbeitung zu journalistischen Zwecken) auch für die Bereiche auszugestalten, die nicht Gegenstand der Mediengesetze der Länder sind. Damit etwa Blogger und andere freie Journalisten rechtssicher arbeiten können, soll diese Regelungslücke zeitnah geschlossen werden. Angesichts der Bedeutung und Komplexität des Vorhabens wird dies nun aber im Rahmen eines separaten Gesetzgebungsverfahrens erfolgen, um das ansonsten sehr technische Anpassungsgesetz mit seinen zahlreichen Änderungsartikeln nicht zu überfrachten.
Das 2. DSAnpUG ist von Seiten des Bundesrates zustimmungsbedürftig und tritt am Tag nach der Verkündung im Bundesgesetzblatt in Kraft.

Siehe hierzu:
https://www.bundestag.de/dokumente/textarchiv/2019/kw26-de-datenschutz-649218

BSI-Empfehlung für sichere Konfiguration von MS-Office-Produkten

Büroanwendungen werden wegen ihrer großen Verbreitung und Angriffsfläche häufig als Angriffsweg genutzt, beispielsweise um mittels Makros in Office-Dokumenten Schadsoftware zu verbreiten und auf Zielsystemen auszuführen. Mit einer wohlüberlegten Konfiguration dieser Produkte kann das Risiko der Ausnutzung von Standardfunktionen oder Schwachstellen minimiert werden.
Das BSI hat für den Einsatz auf dem Betriebssystem Microsoft Windows sieben Cyber-Sicherheitsempfehlungen für eine sichere Konfiguration von Microsoft Office 2013/2016/2019 erstellt. Diese behandeln zum einen übergreifende Richtlinien für Microsoft Office, zum anderen Richtlinien für sechs häufig genutzte Microsoft Office-Anwendungen.
Hauptaugenmerk dieser im Mai 2019 veröffentlichten BSI-Empfehlung liegt auf dem Einsatz von Microsoft Office 2013/2016/2019 in mittelgroßen bis großen Organisationen, in denen die Endsysteme mit Gruppenrichtlinien in einer Active Directory-Umgebung verwaltet werden.

Quelle: Bundesamt für Sicherheit in der Informationstechnik

Hinweispflichten bei Auskunftsbegehren

Frage des GDD-Erfa-Kreises Coburg:
Wenn eine betroffene Person bei einer Firma einen Auskunftsanspruch z.B. per E-Mail geltend macht, muss die betroffene Person dann gem. Art. 13 DS-GVO darauf hingewiesen werden, dass die in der E-Mail angegebenen Daten zur Beantwortung der Auskunft verarbeitet werden? Wenn ja, reicht es dann den Betroffenen bei Beantwortung der Auskunft darauf hinzuweisen oder muss dies gleich nach dem Eingang der E-Mail die Informationen erhalten? Wie lange sollten Auskunfts-Mails zum Nachweis aufbewahrt werden? Wir denken eine Frist von drei Jahren aufgrund etwaiger Rechtsansprüche sollte ausreichend sein.

Antwort des BayLDA:
Die Informationen nach Art. 13 DS-GVO müssen bei Erhebung zur Verfügung gestellt werden. Nach nicht abschließend geklärt ist, was unter Erhebung in diesem Zusammenhang zu verstehen ist. Weiterhin müssen nach Art. 12 Abs. 1 DS-GVO geeignete Maßnahmen zur Erfüllung der Transparenzpflichten getroffen werden. Hieraus lässt sich ableiten, dass praxisgerechte Lösungen getroffen werden können. Es wird dazu voraussichtlich eine Konkretisierung der DSK geben. Bis auf weiteres halten wir es für ausreichend, wenn die Informationen bei einer zeitnahen Beantwortung mit der Antwort-E-Mail gegeben werden. Für die Aufbewahrung von Auskunfts-E-Mails gibt es derzeit noch keine Festlegungen. Wir halten 3 Jahre für ausreichend.

Datenschutzkonforme E-Mail-Weiterleitung bei Abwesenheit oder Ausscheiden aus dem Betrieb

Die LfDI der Hansestadt Bremen widmet sich in einer Orientierungshilfe einer Fragestellung, die sich in der Praxis sehr oft stellt und mit der der betriebliche Datenschutzbeauftragte oft konfrontiert wird.
Wie ist die richtige Vorgehensweise für einen Betrieb und Unternehmen im Hinblick auf den E-Mail-Account eines Beschäftigten, wenn diese Person vorübergehend oder länger abwesend ist oder aus dem Betrieb ausgeschieden ist?
Als relevante Vorschriften der DS-GVO und des BDSG werden von der LfDI der Hansestadt Bremen Artikel 6 Absatz 1 lit. b DS-GVO beziehungsweise § 26 Absatz 1 Satz 1 BDSG zu genannt. Danach dürfen personenbezogene Daten eines oder einer Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies unter anderem für dessen Durchführung oder Beendigung erforderlich ist.
Die Orientierungshilfe spielt bei der Vorstellung der empfohlenen Lösung verschiedene Szenarien durch und stellt für jede der Konstellationen eine datenschutzkonforme Vorgehensweise vor.

Quelle: LfDI Hansestadt Bremen

BvD gründet Dachverband für Datenschutzbeauftragte

Die DS-GVO, die seit dem 25. Mai 2018 wirksam ist, bietet einen modernisierten, auf dem Prinzip der Rechenschaftspflicht beruhenden Handlungsrahmen für die Überprüfung der Einhaltung der Datenschutzvorschriften in Europa. Den Kern dieser neuen Rechtsgrundlage sind für viele Einrichtungen Datenschutzbeauftragte (DSB), die die Einhaltung der Bestimmungen der DS-GVO erleichtern. Nach der DS-GVO sind Verantwortliche und Auftragsverarbeiter unter bestimmten Voraussetzungen verpflichtet, einen DSB zu ernennen. Diese Pflicht besteht für alle Behörden und öffentlichen Stellen (unabhängig von der Art der verarbeiteten Daten) wie auch für sonstige Einrichtungen, die – als Kerntätigkeit – systematisch und in großem Umfang Einzelpersonen überwachen oder in großem Umfang besondere Kategorien von personenbezogenen Daten verarbeiten.

Das dem DSB zugrundeliegende Konzept ist nicht neu. Wenngleich nach der Richtlinie 95/46/EG keine Einrichtung zur Ernennung eines DSB verpflichtet war, hat sich die Praxis der Ernennung eines DSB in zahlreichen Mitgliedstaaten im Laufe der Jahre immer mehr verbreitet.

„Betriebliche Datenschutzbeauftragte sind wichtige Akteure zur Einhaltung datenschutzrechtlicher Bestimmungen“, sagte BvD-Vorstandsvorsitzender Thomas Spaeing.

„Als Datenschutzexperten stellen sie die unternehmerische Handlungsfähigkeit unter der DS-GVO sicher und sorgen zugleich dafür, dass die Verbraucher- und Bürgerrechte beim Datenschutz eingehalten werden. Das entlastet auch die nationalen Datenschutz-Aufsichtsbehörden.“

In Deutschland müssen Unternehmen, bei denen mehr als zehn Personen ständig mit der Verarbeitung personenbezogener Daten betraut sind, einen Datenschutzbeauftragten benennen. „Auch ohne Benennungspflicht müssen die Betriebe die Anforderungen der DSGVO vollumfänglich erfüllen“, erläutert Spaeing. „Aber gerade in kleinen und mittleren Betrieben fehlt dafür intern meist das Knowhow.“

Der BvD ist Initiator des jüngst gegründeten EU-Dachverbands für Datenschutzbeauftragte. Der „European Federation of Data Protection Officers (EFDPO)“ ist am 7.Juni 2019 in Berlin gegründet worden. Neben dem BvD nationale Verbände für Datenschutzbeauftragte aus Österreich, Frankreich, Portugal, Tschechien, der Slowakei, Griechenland und Liechtenstein. Hauptziel der Gründung ist es, die Datenschutzbeauftragten der EU-Mitgliedsstaaten miteinander zu vernetzen, gemeinsame Standards zu entwickeln und die Interessen der in Brüssel zu vertreten. Dabei soll Datenschutz als Wettbewerbs- und Standortvorteil für Europa gestärkt werden. Arbeitssitz des neuen Verbandes ist Brüssel.

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

Beschwerde gegen personalisierte Online-Werbung

Gemeinsam mit elf weiteren Menschenrechts- und Digitalrechtsorganisationen aus neun EU-Staaten reicht das Netzwerk Datenschutzexpertise im Rahmen einer Kampagne eine Beschwerde gegen Google und andere Anbieter personalisierter Online-Werbung ein, wegen Verstößen gegen die Regeln der Datenschutz-Grundverordnung, u. a. zu Zweckbindung, Transparenz, Datensparsamkeit, die Pflicht zu technisch-organisatorischen Sicherungsmaßnahmen, das Verbot automatisierter Entscheidungen und den Schutz sensitiver Daten.
Die Beschwerden markieren den Beginn der Kampagne #StopSpyingOnUs. Ziel der Kampagne ist es, die Öffentlichkeit über eine anhaltende, massive Datenschutzverletzung zu informieren, die alle Nutzerinnen und Nutzer des Internets betrifft, und bei den europäischen Datenschutzbehörden darauf hinzuwirken, deren Möglichkeiten zu nutzen, um diese Praktiken zu beenden

„Die personalisierte Online-Werbung verstößt gegen praktisch alle geltenden Datenschutzprinzipien, u. a. Zweckbindung, Transparenz, Datensparsamkeit, die Pflicht zu technisch-organisatorischen Sicherungsmaßnahmen, das Verbot automatisierter Entscheidungen oder den Schutz sensitiver Daten. Der hoch lukrative Missbrauch unserer Internet-Nutzungsdaten für Werbezwecke durch Google sowie durch andere Unternehmen, die sich im Interactive Advertising Bureau – IAB – organisiert haben, findet seit Jahren statt und kann und muss gestoppt werden. Mit der Datenschutzgrundverordnung besteht nun ein wirksames Instrument.“, so Thilo Weichert vom Netzwerk Datenschutzexpertise.

Quelle: Netzwerk Datenschutzexpertise

Maximale Datensparsamkeit bei Online-Terminen und Umfragen

Vielen kennen und schätzen den Terminplaner des Deutschen Forschungsnetzes oder den dudle-Dienst der TU Dresden als datenschutzfreundlichere Variante zum Platzhirsch „doodle“.
Mit einer eigenen Online-Lösung für die Terminsfindung und kleinere Umfragen schickt der Bielefelder Verein ein Tool ins Rennen, das sogar noch datensparsamer funktioniert als die beiden oben genannten Alternativen.
Dazu hat sich Digitalcourage e.V. des offenen Quellcodes des Tools Framadate von Framasoft bedient und dieses noch weiter im Hinblick auf Datensparsamkeit optimiert.

Das Online-Tool der Bielefelder speichert weder persönliche Daten, noch erstellt es irgendwelche Log-Dateien. Der Webserver des Terminplaners speichert gar keine Access-Logs. Auch die Angabe einer E-Mail-Adresse ist optional. Natürlich muss sich der Nutzer dann zumindest ein Bookmark für die erstelle Umfrage anlegen, um diese wiederzufinden.

Quelle: Digitalcourage e.V.