Datenschutz
newsbox

Ausgabe
2
2019

DATAKONTEXT

Editorial

Der Passwortschutz eines IT-Systems soll gewährleisten, dass nur solche Benutzer einen Zugriff auf die Daten und IT-Anwendungen erhalten, die eine entsprechende Berechtigung nachweisen. Unmittelbar nach dem Einschalten des IT-Systems muss der Berechtigungsnachweis erfolgen. Kann der Benutzer die erforderliche Berechtigung nicht nachweisen, so verhindert der Passwortschutz den Zugriff auf das IT-System (BSI IT-Grundschutz – M 4.1 Passwortschutz für IT-Systeme)

Nach "M 2.11 Regelung des Passwortgebrauchs BSI IT-Grundschutz" müssen Vorgaben für die Passwortgestaltung immer einen praktikablen Kompromiss zwischen folgenden Sicherheitszielen darstellen:

- Die Zeichenzusammensetzung des Passwortes muss so komplex sein, dass es nicht leicht zu erraten ist.
- Die Anzahl der möglichen Passwörter im vorgegebenen Schema muss so groß sein, dass es nicht in kurzer Zeit durch einfaches Ausprobieren ermittelt werden kann.
- Das Passwort darf nicht zu kompliziert sein, damit der Besitzer mit vertretbarem Aufwand in der Lage ist, es auswendig zu lernen.

Eine der (noch) geltenden Regeln zu Passwortgestaltung und -gebrauch des BSI lautet: "Das Passwort muss regelmäßig gewechselt werden, z. B. alle 90 Tage." Diese Empfehlung wird jedoch immer wieder kritisiert. Der jüngste Vorstoß zur Abkehr von dieser Empfehlung kommt vom LfDI Baden-Württemberg.

Darin wird erläutert, warum eine erzwungene regelmäßige Änderung von Passwörtern als überholt angesehen werden kann. Administratoren wird geraten, ihre Nutzer nicht regelmäßig aufzufordern oder zu zwingen, die Passwörter zu ändern. Stattdessen sollen die Nutzer für sichere Passwörter sensibilisiert werden. Es ist äußerst begrüßenswert, dass sich der LfDI BW dafür einsetzt, diesen alten Zopf abzuschneiden, findet Ihr

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

Abschluss eines AV-Vertrags durch Untätigkeit

Frage des GDD-Erfa-Kreises Würzburg:
Ein Unternehmen (muss und) möchte mit allen Kunden, für die es Datenverarbeitung im Auftrag erbringt, AV-Verträge abschließen. Das Unternehmen hat bereits (zeitig genug vor dem 25.05.2018) allen Kunden eine Vertragsvorlage mit der Bitte um Zeichnung nebst Erläuterungen übersandt. Auf Grund der trotz DS-GVO niedrigen Rücklaufquote von nur 20 Prozent soll nun ein neuer Vorstoß gewagt werden: Es soll ein Erinnerungsschreiben versandt werden. Diesem soll, wegen der erwartet wiederum niedrigen Rücklaufquote, nochmals der AV-Vertrag beigegeben werden (der wegen Leistungsidentität inhaltlich stets passt). Zugleich soll darauf hingewiesen werden, dass der Vertrag als geschlossen betrachtet würde, wenn keine Rückkoppelung binnen einer noch zu bestimmenden Frist erfolgt.

- Ist davon auszugehen, dass die Aufsichtsbehörde damit jedenfalls für Zwecke des Datenschutzes einen AV-Vertrag als geschlossen anerkennt? Dies vor dem Hintergrund, dass die Aufsicht trotz Formerfordernisses bereits hat erkennen lassen, dass ein lediglich per Klick dokumentierter AV-Vertrag für Zwecke des Datenschutzes als geschlossen anerkannt werden könne.
- Falls nein, könnte folgendes zweistufige Verfahren dem Anspruch der Behörde genügen? Im ersten Schritt eine Erinnerung nebst nochmaliger Übersendung des AV-Vertrages. Darin die nochmalige Bitte um Abschluss und Ankündigung, dass bei Verstreichenlassen einer weiteren Gelegenheit zum AV-Schluss dieser in der beigegebenen Form als geschlossen betrachtet würde.

Antwort BayLDA:
Es ist problematisch, beim bloßen Nichtreagieren des Auftraggebers von einem abgeschlossenen AV-Vertrag auszugehen. Immerhin erfordert ein Vertrag zwei Willenserklärungen. Allerdings gibt es im Handelsrecht mit dem sog. kaufmännischen Bestätigungsschreiben (kBS) eine rechtlich anerkannte Konstellation, bei der Schweigen als Willenserklärung gilt, so dass das Schweigen in diesem (Ausnahme-)Fall als Willenserklärung einzustufen ist. Allerdings hat das kBS eine Reihe von Voraussetzungen, nämlich:

- Der Empfänger muss Kaufmann sein oder zumindest in größerem Umfang am Geschäftsleben teilnehmen. Der Absender muss dagegen zwar nicht zwingend Kaufmann sein, wohl aber einem solchen vergleichbar am Verkehr teilnehmen (BGHZ 40, 42 ff).
- Es müssen tatsächlich Vertragsverhandlungen dem Bestätigungsschreiben vorangegangen sein.
- Das kaufmännische Bestätigungsschreiben muss alsbald nach den Vertragsverhandlungen abgeschickt werden, so dass der Empfänger auf das Eintreffen vorbereitet ist.
- Das Schreiben muss den früheren Vertragsschluss unter Wiedergabe des Vertragsinhaltes bestätigen.
- Selbstverständlich muss das Schreiben dem Empfänger auch zugehen (vgl. § 130 BGB).
- Der Absender muss der Meinung sein, dass der Inhalt des Schreibens der Vereinbarung entspricht oder nur solche Abweichungen enthält, die der Empfänger billigt (Redlichkeit des Absenders ist also erforderlich).
- Der Empfänger darf nicht unverzüglich widersprochen haben.

Ein KBS setzt also regelmäßig voraus, dass Vertragsverhandlungen vorangegangen waren, und deshalb jedenfalls ein geschäftliches Gespräch über den schriftlich "bestätigten" Vorgang stattgefunden haben muss. Der Empfänger eines kBS braucht allerdings dann nicht zu widersprechen, wenn sich der Inhalt des Schreibens so erheblich von dem Verhandlungsergebnis entfernt, dass der Absender mit dem Einverständnis des Empfängers redlicherweise nicht rechnen konnte."
Nach unserer Auffassung ist die datenschutzrechtliche Frage, ob ein AV-Vertrag wirksam abgeschlossen wurde, gleichlaufend zu behandeln mit der Frage, ob in zivilrechtlicher Hinsicht (unter Berücksichtigung der Rechtsfigur des kaufm. Bestätigungsschreibens) ein Vertrag zustande gekommen ist oder nicht. Das würde bedeuten: Nur wenn die o.g. zivilrechtlich-handelsrechtlichen Voraussetzungen des kBS erfüllt sind, würden wir auch datenschutzrechtlich von einem wirksamen AV-Vertrag i.S.v. Art. 28 DS-GVO ausgehen. Dies nachzuweisen obliegt den Beteiligten.

Umgang mit Datenpannen nach Art. 33 und 34 DS-GVO

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 offen zu legen, sie müssen auch geeignete Hilfestellungen zur Verhinderung schwerwiegender Folgen anbieten.
Eine Verletzung des Schutzes personenbezogener Daten kann – wenn nicht rechtzeitig und angemessen reagiert wird – einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person.

Leider existiert zu diesem Thema noch kein abgestimmtes Papier der Datenschutzkonferenz (DSK). Aus der Feder des BayLDA existiert ein Kurzpapier, welches jedoch viele Fragen offen lässt. Weitaus umfangreichere Informationen und Handlungsempfehlungen enthält ein Papier des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit zum Thema Data-Breach-Meldungen nach Art. 33 DS-GVO. Das Papier befasst sich mit Fragen wie:

- Was ist eine Verletzung des Schutzes personenbezogener Daten?
- Anhand welcher Kriterien kann der Verantwortliche das Risiko bestimmen?
- Wie sollte die Information der Betroffenen erfolgen?
- Beispiels-Fälle für eine Meldung nach Art. 33 DS-GVO
- Wann ist eine Meldung rechtzeitig?

Möglichkeiten der Identitätsüberprüfung bei elektronischem Auskunftsersuchen

Gegenüber öffentlichen und nicht-öffentlichen Stellen haben Betroffene nach Art. 15 der Datenschutz-Grundverordnung (DS-GVO) das Recht auf Auskunft über die zu Ihrer Person gespeicherten Daten und über weitere Informationen.
Dabei dürfte die persönliche Vorsprache vor Ort bei dem Verantwortlichen eher die Ausnahme bilden, sodass sich insbesondere bei elektronische getätigten Auskunftsbegehren die Frage der Identitätsüberprüfung stellt. Es kann sein, dass in Einzelfällen zur Legitimation die Kopie eines Personaldokuments verlangt wird, um eine eindeutige Zuordnung der gespeicherten Daten zu der Person des Betroffenen vorzunehmen und missbräuchliche Auskunftsbegehren – auch im Interesse des Betroffenen – zu verhindern.
Welche empfehlenswerten Möglichkeiten Verantwortlichen bei der Identitätsprüfung zur Verfügung stehen, stellt eine neue Publikation des LfDI BW vor. Dabei wird zwischen schriftlichen Anträgen, telefonischen Anträgen, Anträgen, die per E-Mail eingehen und Anträgen über ein Nutzerkonto unterschieden. Der Autor (Dr. Ronald Petrlic, Referent beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg) geht dankenswerterweise auch auf die Frage ein, auf welchem Wege die Auskunft schließlich erteilt werden sollte, wenn die Auskunft nicht schriftlich per Post erfolgt.
Zum Auskunftsrecht der betroffenen Person nach Art. 15 DS-GVO existiert ebenfalls ein DSK-Papier (Kurzpapier Nr. 6), welches auf der Seite des DSK abgerufen werden kann.

Quelle: LfDI BW

Bundeskartellamt beschränkt das Zusammenführen von Nutzerdaten

Das Bundeskartellamt hat dem Unternehmen Facebook weitreichende Beschränkungen bei der Verarbeitung von Nutzerdaten auferlegt.
Nach den Geschäftsbedingungen von Facebook können Nutzer das soziale Netzwerk bislang nur unter der Voraussetzung nutzen, dass Facebook auch außerhalb der Facebook-Seite Daten über den Nutzer im Internet oder auf Smartphone-Apps sammelt und dem Facebook-Nutzerkonto zuordnet. Alle auf Facebook selbst, den konzerneigenen Diensten wie z.B. WhatsApp und Instagram sowie den auf Drittwebseiten gesammelten Daten können mit dem Facebook-Nutzerkonto zusammengeführt werden.
Die Entscheidung des Amtes erfasst verschiedene Datenquellen:

(i) Künftig dürfen die zum Facebook-Konzern gehörenden Dienste wie WhatsApp und Instagram die Daten zwar weiterhin sammeln. Eine Zuordnung der Daten zum Nutzerkonto bei Facebook ist aber nur noch mit freiwilliger Einwilligung des Nutzers möglich. Wenn die Einwilligung nicht erteilt wird, müssen die Daten bei den anderen Diensten verbleiben und dürfen nicht kombiniert mit den Facebook-Daten verarbeitet werden.

(ii) Eine Sammlung und Zuordnung von Daten von Drittwebseiten zum Facebook-Nutzerkonto ist in der Zukunft ebenfalls nur noch dann möglich, wenn der Nutzer freiwillig in die Zuordnung zum Facebook-Nutzerkonto einwilligt.

Fehlt es bei den Daten von den konzerneigenen Diensten und Drittwebsites an der Einwilligung, kann Facebook die Daten nur noch sehr stark eingeschränkt sammeln und dem Nutzerkonto zuordnen. Entsprechende Lösungsvorschläge hierfür muss Facebook erarbeiten und dem Amt vorlegen.

Nach der Bewertung des Bundeskartellamts verstoßen die Nutzungsbedingungen und die Art und der Umfang der Sammlung und Verwertung der Daten durch Facebook zu Lasten der Nutzer gegen europäische Datenschutzvorschriften. Das Bundeskartellamt hat hinsichtlich der datenschutzrechtlichen Fragestellungen eng mit führenden Datenschutzbehörden zusammengearbeitet.
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit wertete das Urteil als "Wegweisende Entscheidung des Bundeskartellamtes zu Facebook". Nach Ansicht des BfDI verstoße das aktuelle Geschäftsmodell von Facebook in mehreren Punkten gegen die hiesigen datenschutzrechtlichen Vorschriften. Gerade die Tatsache, dass Einwilligungen als wesentliche Grundlage für die meisten Datenverarbeitungen nicht den Vorgaben der DSGVO entsprechen, habe er schon mehrfach kritisiert.
Stimmen aus den Reihen der anwaltlicher Datenschutz-Beratung äußerten Kritik am Vorgehen des Bundeskartellamtes. Zum einen wird die Zuständigkeit des Bundeskartellamts in dieser Frage kritisch hinterfragt, zum anderen wird angeführt, dass durch das Vorgehen des Bundeskartellamts das Kohärenzverfahren nach der DSGVO und, in Streitfällen zwischen Aufsichtsbehörden, die Entscheidungsbefugnis des Europäischen Datenschutzausschusses übergangen wird.
Die Entscheidung des Bundeskartellamtes ist noch nicht rechtskräftig. Facebook hat die Möglichkeit innerhalb eines Monats Beschwerde gegen die Entscheidung einzulegen, über die dann das Oberlandesgericht Düsseldorf entscheiden würde.

Informationen zum Selbstdatenschutz

Unter Selbstdatenschutz versteht man die durch den Einzelnen zum Schutz seines Rechts auf informationelle Selbstbestimmung ergriffenen technischen, organisatorischen und rechtlichen Maßnahmen. Dazu werden bisher in erster Linie Verhaltensweisen des Einzelnen gezählt, möglichst wenig Ansatzpunkte für eine Erhebung seiner Daten zu bieten. Selbstdatenschutz bedeutet, die Gefahren hinsichtlich von Datenschutz und Datensicherheit kennen zu lernen und selbst aktiv Gegenmaßnahmen zu ergreifen.
Die Bayerische Landeszentrale für neue Medien (BLM) hat zu diesem Thema eine Broschüre mit dem Titel "Selbstdatenschutz! Tipps, Tricks und Klicks" herausgegeben. Die Broschüre "Selbstdatenschutz! Tipps, Tricks und Klicks" gibt Mediennutzern in vier Kapiteln alltagstaugliche Tipps sowie verständlich aufbereitete Hintergrundinformationen für einen selbstbestimmten und kompetenten Umgang mit den eigenen Daten. Die Broschüre richtet sich insbesondere an Eltern und pädagogisch Tätige, die Kinder und Jugendliche bei dem verantwortungsvollen Umgang mit persönlichen Daten unterstützen. Zu jedem Themenschwerpunkt befinden sich in gekennzeichneten Abschnitten auf diesen Adressatenkreis abgestimmte Hinweise.

Interessierte finden weitere Informationen zum Thema auch auf den Seiten des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz. Dort können Interessierte sich darüber informieren, welche Möglichkeiten es gibt, Datenspuren im Internet zu vermeiden, E-Mail-Inhalte durch Verschlüsselung zu schützen oder mit welchen Maßnahmen Anwender Inhalte in Online-Speichern noch vertraulich halten können.

Auftragsverarbeitung und Dreiecksverhältnis

Frage des GDD-Erfa-Kreises Würzburg:
Im vorliegenden Fall beauftragt ein Unternehmen einen Dienstleister damit, personenbezogene Daten zu verarbeiten. In diesem Verhältnis besteht also der Leistungsvertrag. Die jeweiligen personenbezogenen Daten erhält der Auftragnehmer jedoch direkt von einem dritten Unternehmen. Es besteht also ein Dreiecksverhältnis, in dem der kaufmännische Auftraggeber ein anderer ist als der "datenschutzrechtliche Auftraggeber", der die personenbezogenen Daten übermittelt.
Der kaufmännische Auftraggeber, mit dem der Leistungsvertrag besteht und der daher letztlich die Weisung erteilt, weigert sich, einen Vertrag über Auftragsverarbeitung zu zeichnen mit der Begründung, dass das Unternehmen die personenbezogenen Daten gar nicht übermittelt, sondern diese direkt von einem anderen Unternehmen stammen (Beispiel Werbeagentur beauftragt eine Druckerei, einen Prospekt zu drucken. Die personenbezogenen Daten hierfür erhält aber die Druckerei direkt vom Tennisverband, der ansonsten keinerlei Vertragsverhältnis zur Druckerei hat. Dieses besteht nur zwischen der Werbeagentur und der Druckerei. Dies ist nur ein Beispiel, das Dreiecksverhältnis kann noch mit anderen Auftragsverarbeitungen stattfinden).

- Unterstellt, es handelt sich um eine Auftragsverarbeitung i.S.d. § 28 DS-GVO, wie müsste hier vorgegangen werden?
- Zwischen welchen Parteien müsste der Vertrag über Auftragsverarbeitung geschlossen werden?

Antwort BayLDA:
Wir bitten um Verständnis, dass wir nur allgemein antworten können, da es immer auf die konkreten Umstände des Einzelfalls ankommt.
Grundsätzlich gilt, dass der Auftragsverarbeitungsvertrag zwischen dem "Verantwortlichen" und dem "Auftragsverarbeiter" abgeschlossen werden muss. Das heißt, es muss anhand der gesetzlichen Definitionen geprüft werden, wer hier Verantwortlicher ist. Nach der Definition in Art. 4 Nr. 7 DS-GVO ist Verantwortlicher derjenige, der über die Zwecke und Mittel der Datenverarbeitung entscheidet. Ohne dass die Sachverhaltsbeschreibung ausreichend klar ist, könnte es aber durchaus sein, dass im vorliegenden Fall der hier so genannte kaufmännische Auftraggeber als Verantwortlicher einzuordnen ist (also nicht derjenige, von dem die Daten physisch an den Dienstleister fließen). Verantwortlicher kann jedenfalls – so der Europäische Gerichtshof mehrfach – auch jemand sein, der selbst nicht notwendigerweise physisch Zugriff auf die Daten hat; erforderlich ist aber, dass er über die Zwecke (und die wesentlichen Mittel) der Verarbeitung entscheidet. In dem vorgetragenen Beispiel könnte somit durchaus die Werbeagentur als Verantwortlicher anzusehen sein, jedenfalls sofern sie diejenige ist, die entscheidet, dass der Prospekt gedruckt werden soll.
Es fragt sich freilich, ob die Werbeagentur diese Verantwortung übernehmen möchte angesichts der Tatsache, dass sie die Daten augenscheinlich physisch gar nicht besitzt. Möglich wäre es aber unseres Erachtens durchaus, jedenfalls wenn es tatsächlich gewollt ist, dass die Weisungen gegenüber der Druckerei nicht durch den Tennisverband, sondern durch die Werbeagentur erteilt werden.

Steuerberater und Lohnbuchhaltung

Das LDI NRW (http://t1p.de/ewvo) geht im Falle der reinen Lohn- und Gehaltsabrechnung oder bei sonstigen, rein technischen Dienstleistungen auch bei Steuerberatern von einer AV aus. Das BayLDA (http://t1p.de/82g6) hingegen sieht auch bei reiner Lohnbuchhaltung eine eigene Verantwortung der Steuerberater aufgrund des Steuerberaterrechts als gegeben an. Die Bundessteuerberaterkammer weist in Ihrem aktualisierten Leitfaden vom Oktober 2018 (Hinweise für den Umgang mit personenbezogenen Daten durch Steuerberater und Steuerberatungsgesellschaften, Ziffer 7.3) auf den Umstand hin, dass die Einbeziehung eines Berufsgeheimnisträgers (StB, RA, WP, externe Betriebsärzte), Inkassobüros mit Forderungsübertragung, Bankinstitute für den Geldtransfer, Postdienste für den Brieftransport etc. keine Auftragsverarbeitung darstellt. Es handele sich um die Inanspruchnahme fremder Fachleistungen bei einem eigenständig Verantwortlichen. Für die Verarbeitung (einschließlich Übermittlung) personenbezogener Daten müsse eine Rechtsgrundlage gem. Art. 6 DS-GVO gegeben sein, z. B. die Einwilligung der betroffenen Person oder die Wahrung berechtigter Interessen des Verantwortlichen (Kanzlei).
Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit, Baden-Württemberg positioniert sich in seinem am 04.02.2019 veröffentlichten, 34. Tätigkeitsbericht ebenfalls zu dieser Fragestellung. Auf Seite 57, Ziffer 1.10 heißt es wie folgt:
"*Übernimmt ein Steuerberater neben seiner eigentlichen Steuerberatertätigkeit (Hilfe in Steuersachen) zusätzlich weitere Aufgaben, handelt es sich um Auftragsverarbeitung im Sinne des Artikels 28 DS-GVO und bedarf einer entsprechenden Vereinbarung mit dem datenschutzrechtlich verantwortlichen Auftraggeber.*"
Damit stützt der LfDI Baden-Württemberg die Position der LDI NRW in der Frage. Für die Beauftragung des Steuerberaters mit der laufenden Lohn- und Gehaltsabrechnung kommt nach Dafürhalten des LfDI BW datenschutzrechtlich nur eine Auftragsverarbeitung im Sinne des Artikels 28 DS-GVO in Betracht.

Auftragsverarbeitung und Abwicklung von Herstellergarantie

Frage des GDD-Erfa-Kreises Würzburg:
Unternehmen B verkauft hochpreisige Produkte, wofür er Einzelteile der Firma A verarbeitet, z. B. Motoren. Diese Motoren haben eine Werksgarantie. A möchte, dass B die Käuferdaten vom Käufer C an A weitergibt, damit:

a) C sich selbständig im Sachmangelfall an A wenden kann (und A den C gleich zuordnen kann).
b) Sollte sich im Sachmangelfall, z. B. Motor defekt, C an B wenden, gibt B die Daten von C auch an A, damit A direkt mit C in Verbindung treten kann.

Ist in diesen Konstellationen ein Auftragsverarbeitungsvertrag notwendig?

Antwort BayLDA:
Auch dies stellt keinen Fall von Auftragsverarbeitung dar, da B in Fällen, in denen sich Käufer an ihn wenden, die Daten zum Zwecke der Erbringung der Leistungen aus der Herstellergarantie verarbeitet, also insoweit selbst die Zwecke der Datenverarbeitung (eben die Verarbeitung zwecks Erfüllung der Herstellergarantie) festgelegt hat.
Da B somit Verantwortlicher ist, bedarf es für die Übermittlung der Daten des Käufers von B an A einer Rechtsgrundlage nach Art. 6 DS-GVO. Zu prüfen ist zunächst, ob zwischen A und C ein Garantievertrag zustande gekommen ist (dies kann im Einzelfall durchaus sein, erfordert aber einen wirksamen zivilrechtlichen Vertragsschluss hinsichtlich der Garantie zwischen A und C – dies müsste zivilrechtlich geprüft werden, wir als Aufsichtsbehörde können grundsätzlich keine zivilrechtlichen Fragen prüfen). Sofern kein Vertragsschluss zwischen A und C vorliegt, wäre für die Übermittlung eine Einwilligung des Käufers gem. Art. 6 Abs. 1 a) DS-GVO erforderlich.

Erste Sitzung des Europäischen Datenschutzausschusses in 2019

Am Mittwoch (23.01.2019) kamen die Datenschutzbeauftragten der EU-Mitgliedstaaten in Brüssel zu ihrer ersten Sitzung in diesem Jahr zusammen. Bei der Sitzung des Europäischen Datenschutzausschusses (EDSA) wurden nach Angaben des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), Ulrich Kelber, erneut wichtige Weichen für den europäischen Datenschutz gestellt. Themen waren insbesondere der EU-US Privacy Shield, Leitlinien zur Zertifizierung und die Verbesserung der Kommunikation mit Social-Media-Anbietern bei Datenschutzvorfällen.

Überprüfung des Privacy Shield

Ein wichtiger Tagesordnungspunkt war der Beschluss des Berichts zur 2. Jährlichen Gemeinsamen Überprüfung des Privacy Shield. In diesem finden sich Anregungen, wie das Abkommen weiter verbessert werden kann. Denn auch wenn die US-Behörden wichtige Schritte unternommen haben, um die Vorgaben des Privacy Shield effektiver zu überprüfen, bleiben nach wie vor gewichtige Kritikpunkte, so der BfDI. Nach wie vor fehlt eine dauerhafte Besetzung der Ombudsperson und die Offenlegung ihrer Befugnisse gegenüber den Sicherheitsbehörden. Hierzu erklärte Kelber: "Es bleibt nach wie vor zweifelhaft, ob der Ombudspersonmechanismus in der Praxis das erforderliche Maß an Rechtschutz gewährt. Ich erwarte von unseren amerikanischen Freunden, dass sie hier für die nötige Klarheit sorgen."

Voraussetzungen für die Zertifizierung nach DS-GVO schaffen

Weiterer Punkt auf der Tagesordnung war die Verabschiedung der Guidelines on Certification. Die Leitlinien sollen Anhaltspunkte für die Ausgestaltung von Zertifizierungsprozessen nach der DS-GVO geben. Gemeinsam mit den bereits im Dezember vergangenen Jahres verabschiedeten Guidelines on Accreditation dienen beide Papiere als wichtige Orientierungshilfen. Es liegt nun ein weiteres Puzzleteil vor, um auch in Deutschland das Verfahren zur Schaffung der Voraussetzungen für die Zertifizierung des DSGVO-konformen Datenschutzes endlich finalisieren zu können.

Kommunikation zwischen Aufsichtsbehörden und Social-Media-Anbietern

Schließlich hat sich der EDSA auf Anregung Deutschlands im Nachgang des hiesigen Doxxing-Skandals auch mit der Frage befasst, wie die aufsichtsrechtliche Kommunikation mit Social-Media-Anbietern und anderen IT-Unternehmen verbessert und vor allem beschleunigt werden kann. Ziel soll es sein, bei Datenschutzvorfällen schneller reagieren zu können, um negative Auswirkungen für die Betroffenen möglichst gut zu minimieren. Hierzu einigte man sich darauf, gemeinsam technische und organisatorische Maßnahmen zu erörtern, um in Eilfällen eine unmittelbare Kontaktaufnahme mit den verantwortlichen Stellen zu ermöglichen. Die deutschen Datenschutzbehörden werden dazu einen Vorschlag vorlegen.

An die DS-GVO angepasste Standardvertragsklauseln

Frage des GDD-Erfa-Kreises Würzburg:
Wird es eine auf die DS-GVO angepasste Variante der EU-Standvertragsklauseln geben?

Antwort BayLDA:
Die zuletzt vernommenen Signale der Europäischen Kommission waren diesbezüglich nicht ganz klar. Zunächst sah es so aus, als würde die Kommission wohl in absehbarer Zeit zwar eine gewisse Anpassung der Standardvertragsklauseln an die DS-GVO planen, allerdings scheint sich dies derzeit zu verzögern. Wohl eher nicht damit zu rechnen ist, dass die Kommission in absehbarer Zeit den Standardvertrag für Übermittlungen an Auftragsverarbeiter um die Anforderungen an einen Auftragsverarbeitungsvertrag nach Art. 28 DS-GVO ergänzt. Mithin muss in solchen Fällen derzeit außer dem Standardvertrag zur Auftragsverarbeitung gemäß Kommissionsbeschluss 2010/87/EU immer noch ein zusätzlicher Vertrag zur Auftragsverarbeitung nach Art. 28 DS-GVO abgeschlossen werden. Es sei aber darauf hingewiesen, dass die bisher existierenden Standardvertragsklauseln gemäß der ausdrücklichen Regelung in Art. 46 Abs. 5 DS-GVO auch unter der DS-GVO fortgelten. Insofern müssen Unternehmen also nicht befürchten, dass die "alten" Vertragstexte unzureichend wären.

50 Millionen Bußgeld für Google

Was mit der DS-GVO stets befürchtet wurde, ist nun erstmalig Realität geworden: Die französische Aufsichtsbehörde CNIL hat nun gegen Google ein erstes hohes Bußgeld ausgesprochen.

Ausgangspunkt des Verfahrens: Beschwerden von Verbänden
Am 25. und 28. Mai 2018 erhielt die CNIL zwei Kollektivbeschwerden des Verbandes None Of Your Business (NOYB) und des Vereins La Quadrature du Net (LQDN) gemäß Art. 80 DS-GVO. In kumulativer Weise stehen diese Beschwerden für 9.974 Personen. In seiner Beschwerde erklärt der Verband NOYB insbesondere, dass Nutzer von Android-Mobilgeräten die Datenschutzbestimmungen von Google und die Allgemeinen Geschäftsbedingungen akzeptieren müssten oder alternativ den Service nicht nutzen könnten. Der Verband LQDN ist der Ansicht, dass Google unabhängig vom verwendeten Endgerät keine gültigen Rechtsgrundlagen für die Durchführung der Verarbeitung personenbezogener Daten zum Zwecke der Verhaltensanalyse und für das Targeting von Werbung hat.

1. Verstoß: Mangelnde Transparenz i.S.d. Art. 12-14 DS-GVO
Angriffspunkt in der Beschwerde ist, dass die Informationen, die das Unternehmen den Nutzern zur Verfügung stellt, die in Art. 12 DS-GVO festgelegten Ziele der Zugänglichkeit, Klarheit und des Verständnisses nicht erfüllen und dass bestimmte Informationen, die in Art. 13 DS-GVO verpflichtend vorgeschrieben sind, den Nutzern nicht zur Verfügung gestellt werden. Tatsächlich sind die Informationen, die Einzelpersonen gemäß Art. 13 DS-GVO offengelegt werden müssen, übermäßig in mehreren Dokumenten verstreut: Sowohl in den Datenschutzrichtlinien als auch in den Nutzungsbedingungen, die während der Kontoerstellung angezeigt werden, sowie Privacy rules, die in einem zweiten Zeitpunkt durch anklickbare Links im ersten Dokument zugänglich sind. Diese verschiedenen Dokumente enthalten Schaltflächen und Links, die aktiviert werden müssen, um zusätzliche Informationen zu erhalten. Eine solche aktive Wahl führt zu einer Fragmentierung von Informationen, so dass der Benutzer die zum Zugriff auf die verschiedenen Dokumente erforderlichen Klicks vervielfachen muss. Die betroffene Person muss dadurch mit hohem Aufwand eine Vielzahl von Informationen einholen, bevor sie die relevanten Absätze identifizieren kann. Die vom Benutzer zu leistene Arbeit geht noch weiter, da er die gesammelten Informationen immer noch abgleichen und vergleichen muss, um zu verstehen, welche Daten gemäß den verschiedenen Einstellungen erfasst werden, die er möglicherweise ausgewählt hat.

2. Verstoß: Keine rechtskonforme Einwilligung für Anzeigenpersonalisierung
Auch im Hinblick auf die Erwähnung der Rechtsgrundlage der personalisierten Werbung herrscht Unklarheit und wenig Nachvollziehbarkeit. In der Datenschutzerklärung des Unternehmens heißt es zunächst: "Wir bitten Sie um Ihre Einwilligung, Ihre Daten für bestimmte Zwecke zu verarbeiten, und Sie können Ihre Einwilligung jederzeit widerrufen. Zum Beispiel bitten wir Sie, um Ihre Einwilligung personalisierte Services wie Anzeigen bereitzustellen." (Übersetzung der Datenschutzerklärung). Die hier gewählte Rechtsgrundlage scheint also die Einwilligung zu sein. Google baut jedoch nicht ausschließlich auf die Einwilligung als Rechtsgrundlage, sondern stellt parallel weiter auf berechtigte Interesse ab. Auf dieser Grundlage werden insbesondere Marketingmaßnahmen und Werbung durchgeführt, um die Dienste von Google bei den Nutzern bekannt zu machen und um eine große Anzahl der Dienstleistungen für Benutzer frei verfügbar zu machen. Im Ergebnis kommt die CNIL dazu, dass die Einwilligung, auf die sich das Unternehmen zur Personalisierung von Werbung stützt, nicht wirksam eingeholt wird. Die Einwilligung wird vom Betroffenen weder in informierter Weise noch als ausdrückliche Willensbekundung erteilt. Eine pauschale Einwilligung in alle in der Datenschutzerklärung genannten Fälle kann die Anforderungen an eine für einen konkreten Fall erteilte Einwilligung nämlich nicht erfüllen.

Was führte zu der enormen Bußgeldhöhe?
Google hält eine Geldbuße von 50 Millionen Euro für unverhältnismäßig. Das Unternehmen ist seit 2015 eine hundertprozentige Tochtergesellschaft von ALPHABET und erzielte im Jahr 2017 einen Umsatz von 109,7 Milliarden US-Dollar (rund 96 Milliarden Euro). Dementsprechend wäre ein Bußgeld gem. Art. 83 DS-GVO in Höhe von bis zu 3,84 Milliarden Euro zulässig gewesen.
Für die Festsetzung der Bußgeldhöhe war laut der CNIL primär die besondere Natur der Verstöße, die in der Rechtmäßigkeit der Verarbeitung sowie in den Transparenz- und Informationspflichten festgestellt wurden, maßgebend. Unstrittig ist Art. 6 DS-GVO eine zentrale Bestimmung des Schutzes personenbezogener Daten. Transparenz- und Informationspflichten sind auch insofern unabdingbar, als sie die Ausübung der Rechte der Menschen beeinflussen und ihnen so die Kontrolle über ihre Daten ermöglichen. In dieser Hinsicht gehören sowohl Art. 6 DS-GVO als auch Art. 12 und 13 DS-GVO zu den Bestimmungen, deren Unkenntnis nach Art. 83 Abs. 5 DS-GVO am stärksten geahndet werden kann. Hinzu kam der Umstand, dass die festgestellten Mängel bis heute andauern. Es handelt sich weder um ein kurzfristiges Missverständnis der Rechtspflichten des Unternehmens noch um einen gewöhnlichen Verstoß, den der Verantwortliche seit der behördlichen Prüfung spontan beendet hätte. Schließlich ist die Schwere der Verstöße zu bewerten, insbesondere im Hinblick auf den Zweck der Behandlungen, ihren Umfang und die Anzahl der betroffenen Personen. Nach Ansicht des Unternehmens sind nur 7 Prozent ihrer Nutzer direkt betroffen, dennoch ist die Anzahl der betroffenen Personen in absoluten Zahlen besonders wichtig. In Anbetracht des Umfangs der Datenverarbeitung – insbesondere der Personalisierung von Werbung – und der Anzahl der betroffenen Personen zeigt die Aufsichtsbehörde, dass die zuvor festgestellten Mängel von besonderer Bedeutung sind. Mangelnde Transparenz in Bezug auf diese weitreichenden Behandlungen sowie das Fehlen einer gültigen Einwilligung des Nutzers zur Personalisierung von Werbung stellen erhebliche Verstöße gegen den Schutz ihrer Privatsphäre dar.

Fazit

Im Ergebnis hält die französische Aufsichtsbehörde eine finanzielle Strafe bis zu 50 Millionen Euro für gerechtfertigt, ebenso eine ergänzende Werbesanktion aus den gleichen Gründen. Berücksichtigt werden dabei auch die herausragende Stellung des Unternehmens auf dem Markt für Betriebssysteme, die Schwere der Mängel und das Interesse, welches diese Entscheidung bei der Information der Öffentlichkeit darstellt. Es wäre nicht überraschend, dass Google den Bußgeldbescheid der CNIL gerichtlich überprüfen lassen wird. Bei dieser Bußgeldhöhe wird dies wohl die logische Reaktion sein, die keine Scheu vor weiteren Kosten für Gericht und Anwälte kennt.

Quelle: *dataagenda.de*

Vereinigtes Königreich gilt ab dem 30.03.2019 als Drittland

Die Europäische Kommission teilte bereits 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.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz fasst auf seiner Internetseite zusammen, welche Bestimmungen verantwortliche Stellen in der EU, und damit auch in Rheinland-Pfalz berücksichtigen müssen:

- Im Informationsblatt zur Datenverarbeitung und in der Datenschutzerklärung einer Website ist gemäß Art. 13 Abs. 1 lit. f bzw. Art. 14 Abs. 1 lit. f DS-GVO über die Datenübermittlung in ein Drittland zu informieren.
- Wenn eine betroffene Person von ihrem Auskunftsrecht Gebrauch macht, ist sie gemäß Art. 15 Abs. 1 lit. c, Abs. 2 DS-GVO auch über die Datenübermittlung in Drittländer zu beauskunften.
- Im Verzeichnis von Verarbeitungstätigkeiten sind Datenübermittlungen in Drittländer, gemäß Art. 30 Abs. 1 lit. d und lit. e DS-GVO bzw. Art. 30 Abs. 2 lit. c DS-GVO, als solche zu bezeichnen und die weiteren in diesem Zusammenhang geforderten Angaben zu machen.
- Ggf. sind Datenschutz-Folgenabschätzungen erstmals durchzuführen oder bereits erfolgte zu überprüfen, soweit es um die Datenübermittlung in das UK als Drittland geht (Art. 35 DS-GVO).

Auch das Information Commissioner's Office (ICO), die unabhängige Datenschutz-Aufsichtsbehörde in Großbritannien informiert auf seiner Internetseite über die Auswirkungen der einzelnen Austritts-Szenarien.

13. Europäischer Datenschutztag 2019 bei der GDD

Zum 13. Europäischen Datenschutztag 2019 hatte sich die GDD auf die Fahnen geschrieben, diejenigen Verantwortlichen im Datenschutz sensibilisieren, die nicht in einer deutschen Niederlassung für einen Schutz personenbezogener durch Beratung und Kontrolle sorgen oder die nicht der deutschen Sprache mächtig sind.
In der GDD-Praxishilfe "Germany's Federal Data Protection Act" wird für ausländische Interessierte das BDSG als nationales Implementierungsgesetz in seinen für die Privatwirtschaft wichtigsten Regelung vorgestellt.
Themen der Praxishilfe sind u.a. die Zulässigkeit der Datenverarbeitung, Restriktionen bei den Betroffenenrechten, der Datenschutzbeauftragte sowie Kompetenzen der Aufsichtsbehörden.
Die Praxishilfe möchte nicht nur Interessierte sensibilisieren, sondern auch einen Beitrag zum aktuellen Stand der nationalen Implementierungsgesetze leisten. Zwar verfügen nicht alle Mitgliedstaaten bereits über ein verabschiedetes Gesetz, es wäre jedoch aus Sicht der GDD wünschenswert, wenn mehr Transparenz hinsichtlich der Implementierungsgesetze bestünde.
Die Praxishilfe kann hier abgerufen werden.

Datenschutz: Arbeitsmaterialsammlung für Lehrende

Laut dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. sind Dozentinnen und Dozenten des BvD seit Anfang 2009 mit Unterrichtskonzepten für die Sekundarstufen I und II bundesweit an Schulen unterwegs, um Schülerinnen und Schülern klare und einfache Verhaltensregeln für den sensiblen Umgang mit ihren persönlichen Daten im Netz näher zu bringen.
Kinder und Jugendliche gehen längst selbstverständlich mit Computer, Smartphones und Tablets um. Dem BvD ist es ein besonderes Anliegen, junge Menschen für mehr Sicherheit im Internet zu sensibilisieren. Die Initiative möchte aufzeigen, wie Schülerinnen und Schüler ihre persönlichen Daten besser schützen können – ohne dabei auf moderne Kommunikationsformen verzichten zu müssen. Dazu hat die Initiative Sensibilsierungsvorträge speziell für junge Internet-User der Sekundarstufen I und II sowie für Klassen an Berufsschulen erarbeitet. Sie bieten Schülerinnen und Schülern klare und einfache Verhaltensregeln für mehr Sicherheit im Netz – ausgerichtet an der Lebenswelt der Kinder und Jugendlichen.
Gemeinsam mit klicksafe wurde aktuell die 3. Auflage des Lehrerhandouts (Arbeitsmaterial zum sensiblen Umgang mit persönlichen Daten im Netz) zu den Vorträgen von "Datenschutz geht zur Schule" erstellt. Die Materialsammlung ist in acht Kapitel aufgeteilt, wobei jedes davon verschiedene Bausteine zu einzelnen Themen enthält. Dabei kann jedes Kapitel unabhängig von den anderen im Unterricht Verwendung finden. Eine Linkliste zu den jeweiligen Kapiteln hilft Thematiken auf sinnvollen Seiten und Portalen zu vertiefen.

Kapitel 1 | Datenschutz, Big Data und Profiling
Kapitel 2 | Mobiles Internet und das Internet der Dinge
Kapitel 3 | Soziale Netzwerke in Schule und Arbeit
Kapitel 4 | Das Recht am eigenen Bild
Kapitel 5 | Passwortschutz und PC Sicherheit
Kapitel 6 | Cybertreffen, Sexting und Selfie
Kapitel 7 | Freizeit – Gaming und Drohnen
Kapitel 8 | Lehrer und Datenschutz

Die Arbeitsblattsammlung "Datenschutz geht zur Schule – Sensibler Umgang mit persönlichen Daten" kann auf bvdnet.de oder auf klicksafe.de kostenfrei als PDF-Datei herunterladen werden.

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

EU und Japan erkennen beiderseits angemessenes Datenschutzniveau an

Die EU und Japan haben bereits am 17. Juli 2018 ihre Gespräche über ein beiderseits angemessenes Datenschutzniveau erfolgreich abgeschlossen. Sie haben sich darauf verständigt, die Datenschutzsysteme der jeweils anderen Seite als "gleichwertig" anzuerkennen, sodass Daten zwischen der EU und Japan sicher fließen können. Die jeweiligen internen Verfahren für die Annahme ihrer Angemessenheitsfeststellung sind nun beendet. Im Falle der EU gehörten dazu die Einholung einer Stellungnahme des Europäischen Datenschutzausschusses sowie die Zustimmung eines Ausschusses, der sich aus Vertretern der EU-Mitgliedstaaten zusammensetzt. Nach dem dieses Verfahren abgeschlossen ist, hat die Kommission den Angemessenheitsbeschluss in Bezug auf Japan angenommen.

Mit dieser Vereinbarung bekräftigen die EU und Japan, dass die Förderung hoher Datenschutzstandards und die Erleichterung des internationalen Handels im digitalen Zeitalter Hand in Hand gehen. Im Rahmen der Datenschutz-Grundverordnung ist ein Angemessenheitsbeschluss der einfachste Weg, um sichere und stabile Datenströme zu gewährleisten.

Die getroffene Vereinbarung sieht die gegenseitige Anerkennung eines gleichwertigen Datenschutzniveaus durch die EU und Japan vor. Nach Annahme werden mit dieser Vereinbarung personenbezogene Daten geschützt, die zu gewerblichen Zwecken übertragen werden, aber auch solche, die zu Strafverfolgungszwecken zwischen den Behörden der EU und Japans ausgetauscht werden, sodass sichergestellt wird, dass bei all diesen Übermittlungen ein hohes Datenschutzniveau zur Anwendung kommt.

Bevor die Kommission ihren Angemessenheitsbeschluss angenommen hat, hat Japan zusätzliche Garantien eingeführt, um zu gewährleisten, dass die aus der EU übermittelten Daten den europäischen Standards entsprechenden Schutzgarantien unterliegen. Diese Garantien umfassen Folgendes:

- **Eine Reihe von Bestimmungen (Ergänzende Vorschriften), die bestimmte Unterschiede zwischen den beiden Datenschutzsystemen ausgleichen werden.** Diese zusätzlichen Garantien werden beispielsweise den Schutz sensibler Daten, die Ausübung individueller Rechte sowie die Bedingungen, unter denen EU-Daten aus Japan in ein anderes Drittland weitergeleitet werden können, stärken. Diese Ergänzenden Vorschriften sind für japanische Unternehmen, die Daten aus der EU einführen, verbindlich und vor der unabhängigen japanischen Datenschutzbehörde (PPC) und den Gerichten durchsetzbar.
- Die japanische Regierung hat der Kommission auch Garantien in Bezug auf den Datenzugriff japanischer Behörden **zu Strafverfolgungszwecken und zu Zwecken der nationalen Sicherheit** zugesagt, damit gewährleistet ist, dass jede Verwendung personenbezogener Daten auf das beschränkt ist, was erforderlich und verhältnismäßig ist und einer unabhängigen Aufsicht sowie wirksamen Rechtsbehelfsmechanismen unterliegt.
- Ein **Verfahren zur Prüfung und Klärung von Beschwerden** von Europäerinnen und Europäern über den Zugriff japanischer Behörden auf ihre Daten. Dieser neue Mechanismus wird von der unabhängigen Datenschutzbehörde Japans verwaltet und überwacht.

Nach zwei Jahren wird eine erste gemeinsame Überprüfung durchgeführt, um das Funktionieren des Rahmens zu bewerten. Dies betrifft alle Aspekte der Angemessenheitsfeststellung, einschließlich der Anwendung der Ergänzenden Vorschriften und der Garantien für den Zugang der Regierung zu den Daten. Die Vertreter des Europäischen Datenschutzausschusses werden sich an der Überprüfung des Datenzugriffs zu Strafverfolgungszwecken und zu Zwecken der nationalen Sicherheit beteiligen. Anschließend wird mindestens alle vier Jahre eine Überprüfung durchgeführt.

Quelle: EU-Kommission