datenschutz-berater.de

45. Jahrgang

DSB 06/2021

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Editorial

Dr. Alexander Golland
Im Schweinsgalopp zum Tele-Daten-Dies-und-Das-Gesetz Seite 169

Stichwort des Monats

Dr. Olaf Koglin
Joint Control von Webseitenbetreibern und „Vendoren" bei Tracking & Co.: Das Branchenmuster von BVDW/IAB Seite 170

Datenschutz im Fokus

Gerhard Deiters
Meldepflichten nach Art. 33 Abs. 1 Satz 1 DSGVO: Abgrenzungsfragen nach dem „Hafnium-Hack" Seite 174

Alexander Weidenhammer und Max Just
Die menschliche Firewall – Der Nutzer als Sicherheitsrisiko? Seite 178

Kathrin Schürmann
Digitales 360-Grad-Feedback und Datenschutz: Was ist zu beachten? Seite 183

Samuel Gail
Übermittlung = Übermittlung? Die begrifflichen Unterschiede in der DSGVO Seite 187

Aktuelles aus den Aufsichtsbehörden

Jannik Krone
Kritik an unverschlüsselten Faxen: Es ist eine Einstellungsfrage Seite 192

Rechtsprechung

Dr. Dominik Sorber
BAG beschränkt Anspruch auf Datenkopie nach Art. 15 Abs. 3 DSGVO Seite 197

Franziska Weber
EuGH-Vorlage zu Anforderungen an spezifischere Normen der Mitgliedstaaten im Sinne des Art. 88 DSGVO Seite 200

■ **Nachrichten** Seite 172 ■ **Service** Seite 204

ISSN 0170-7256

dfv Mediengruppe

Gerhard Deiters

Meldepflichten nach Art. 33 Abs. 1 Satz 1 DSGVO: Abgrenzungsfragen nach dem „Hafnium-Hack“

In der Nacht zum 3. März 2021 veröffentlichte Microsoft kritische Sicherheitsupdates für lokal betriebene Exchange Server, die vier Schwachstellen schließen sollten, die Angreifern eine relativ einfache Möglichkeit eröffneten, auf Daten zuzugreifen und Schadsoftware zu installieren. Die deutschen Datenschutzbehörden veröffentlichten sehr schnell Handlungsempfehlungen und – teilweise voneinander erheblich abweichend – Ansichten, in welchen Fällen eine Meldung nach Art. 33 Abs. 1 Satz 1 DSGVO zu erfolgen habe. Dieser Beitrag zeigt auf, dass die Datenschutzbehörden teilweise zu weitgehende Anforderungen an die Meldepflicht stellen und Unternehmen nicht jeden Verdacht auf einen möglichen Abfluss von Daten zu melden haben.

Ausgangspunkt: Die Proxylogon-Sicherheitslücke und deren Brisanz

Die auf dem Namen „Proxylogon“ getaufte Sicherheitslücke der Exchange Server 2010, 2013, 2016 und 2019 versetzte die IT- und Datenschutz-Welt Anfang März in einen Schockzustand – der Öffentlichkeit besser bekannt unter dem Begriff „Hafnium-Hack“, da die Angriffe im Kern einer chinesischen Hackergruppe mit diesem Namen zugeschrieben werden. Sie sorgte dafür, dass zehntausende lokal betriebene Systeme in Deutschland kurzfristig gepatcht und vom Netz genommen wurden. Das BSI sah sich sogar erstmalig seit 2014 genötigt, die „IT-Bedrohungslage: 4/Rot“ auszusprechen, mittlerweile wurde dies auf „IT-Bedrohungslage: 3/Orange“ und damit „nur“ noch als „geschäftskritisch mit massiven Einschränkungen des Regelbetriebs“ abgeschwächt. Mutmaßlich mehrere tausend Meldungen nach Art. 33 Abs. 1 Satz 1 DSGVO gingen bei den Landesdatenschutzbehörden ein, die hierzu auch in – teilweise abgestufter Form – aufgerufen hatten. Mittlerweile scheint die mediale Präsenz des Themas abzuflauen, wobei von Entwarnung immer noch nicht die Rede sein kann.

Um sich die Brisanz zu vergegenwärtigen, muss man sich u. a. folgende Tatsachen klarmachen: In Endnutzer-Lizenzverträgen für Standardsoftware liest man häufig Formulierungen wie „Die Parteien sind sich einig, dass Software nie mangelfrei ist“. In technischer (nicht zwingend: juristischer) Hinsicht dürfte dies genauso richtig sein, wie die Feststellung, dass die Möglichkeit der Kompromittierung von IT-Systemen praktisch nie ausgeschlossen werden kann. Zumeist sitzt die Sicherheitslücke vor dem Bildschirm, häufig genug gibt es aber auch Sicherheitslücken in der genutzten Software. Nicht umsonst veröffentlichen die Hersteller bekannter Standardsoftware wie Microsoft z. B. für Windows Betriebssysteme oder besagten Exchange Server regelmäßig Sicherheitsupdates. Man kann daher feststellen, dass insbesondere bei komplexerer Software immer Sicherheitslücken bestehen und Systeme vulnerabel sind. Dennoch werden in den wenigsten Fällen, in denen Sicherheitsupdates zur Verfügung gestellt werden, ganze Systeme vom Netz genommen und massenhaft Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Datenschutzbehörden gemacht oder von diesen gefordert. Was ist also das Besondere an der Proxylogon-Sicherheitslücke, die bis März 2021 bereits mindestens zehn Jahre bestand und nachweisbar spätestens ab November 2020 auch ausgenutzt wurde?

Die Brisanz der Proxylogon-Sicherheitslücke beruht auf drei Faktoren:

1. Die Lücke ist sehr einfach auszunutzen: Angriffe können automatisiert gegen eine praktisch unendliche Vielzahl von Systemen gleichzeitig erfolgen und die Angreifer können Schadsoftware in das Active Directory einschleusen, welches auf dem Exchange Server vielfach mit sehr hohen Rechten ausgestattet ist.
2. Weltweit konnte beobachtet werden, dass bis zu einem Bekanntwerden der Sicherheitslücke durch die Veröffentlichung der Sicherheitsupdates durch Microsoft relativ wenige Angriffe gegen offenkundig ausgewählte Ziele registriert wurden, mit Bekanntwerden aber von mehr als zehn bekannten Hackergruppen massenhaft und scheinbar wahllos Angriffe auf am Netz „hängende“ lokal betriebene Exchange Server erfolgten.
3. Aufgrund der Vorbehalte gegen Cloud-Dienste werden in Deutschland verhältnismäßig viele Exchange Server lokal betrieben, zum Zeitpunkt der Zurverfügungstellung der Sicherheitsupdates ca. 57.000.

Unter Ausnutzung der Proxylogon-Sicherheitslücke konnten bzw. können Angreifer den E-Mail-Verkehr abgreifen, Adressbücher auslesen oder Ransomware mit erpresserischer Absicht installieren, die unentdeckt wie tickende Zeitbomben auf tausenden Exchange Servern auf eine Aktivierung warten könnten. Aufgrund der vorstehend genannten massiven Angriffswelle ab Bekanntwerden der Sicherheitslücke teilte das BSI in einer Pressemitteilung vom 5. März 2021 mit, dass davon auszugehen sei, dass zu diesem Zeitpunkt noch nicht gepatchte Exchange Server kompromittiert seien. Dass eine Kompromittierung von

Exchange Servern zumindest potenziell große Mengen und zu einem Teil auch sensible personenbezogene Daten betreffen dürfte, steht außer Frage.

Aussagen zu Meldepflichten durch die Datenschutzbehörden und Empfehlungen

Sowohl dem BSI als auch den Datenschutzbehörden gebührt das Lob, sehr zügig Praxishinweise zum Umgang mit der Proxylogon-Sicherheitslücke veröffentlicht zu haben. Diese wurden auch in zeitlich kurzen Abständen nach Maßgabe neuer Erkenntnisse aktualisiert, wobei die letzten Aktualisierungen von Ende März 2021 stammen.

Sorgen betroffener Unternehmen

Grundsätzlich ist davon auszugehen, dass von der Proxylogon-Sicherheitslücke betroffene Unternehmen zuallererst Sorgen bzgl. der Aufrechterhaltung ihres Geschäftsbetriebs sowie den Schutz ihrer Geschäftsgeheimnisse hatten und auch heute noch haben.

Ein gewichtiger Punkt war allerdings auch die Frage, inwieweit Meldepflichten nach Art. 33 Abs. 1 Satz 1 DSGVO aufgrund der Verletzung des Schutzes personenbezogener Daten zu erfüllen waren. Praktische Bedeutung hat dies bekanntlich aufgrund des Umstandes, dass nach Art. 83 Abs. 4 DSGVO eine empfindliche Geldbuße droht, sofern eine erforderliche Meldung nach Art. 33 Abs. 1 Satz 1 DSGVO nicht, nicht rechtzeitig (unverzüglich, spätestens jedoch 72 Stunden nach Bekanntwerden der Verletzung) oder nicht vollständig (wobei Art. 33 Abs. 4 DSGVO unter bestimmten Umständen auch eine schrittweise Zurverfügungstellung von Informationen gestattet) erfolgt. Darüber hinaus stellt sich auch strategisch die Frage, ob im Hinblick auf die mögliche Schutzwirkung einer Meldung nach §§ 42 Abs. 4, 43 Abs. 4 BDSG eine Meldung erfolgen sollte.

Aussagen der Datenschutzbehörden

Bis Mitte März wurden von fast allen Landesdatenschutzbehörden Aussagen darüber getroffen, ob und wann Meldepflichten nach Art. 33 Abs. 1 Satz 1 DSGVO bestehen. Diese Aussagen sind jedoch im Einzelnen im Umfang als auch inhaltlich alles andere als einheitlich und sind insbesondere im Hinblick auf zukünftig ähnlich gelagerte Fälle zu hinterfragen. Wenn teilweise lediglich darauf verwiesen wird, dass festgestellte Datenschutzverletzungen gemäß Art. 33 Abs. 1 Satz 1 DSGVO zu melden sind, kann man dem schwerlich widersprechen, allerdings stellt sich auch keine Hilfestellung dar. Interessanter ist, dass die Datenschutzbehörden von einer extensiven Auslegung der Meldepflicht seitens der LfD Niedersachsen, dem Sächsischen DSB sowie dem Bayrischen LDA bis zu einer eher zurückhaltenden Annahme einer Meldepflicht durch den LfDI Mecklenburg-Vorpommern offenkundig im Detail verschiedene Ansichten vertreten. Die LfD Niedersachsen geht in ihrem Artikel „Kompromittierte Exchange Server meldepflichtig“ vom 10. März 2021, zuletzt aktualisiert am 23. März 2021, z. B. „davon aus, dass in jedem Fall einer Kompromittierung des Exchange Servers oder eines nicht rechtzeitigen Updates eine Meldung gemäß Art. 33 DSGVO abzugeben ist“. Der LfDI Mecklenburg-Vorpommern hingegen weist in seiner Pressemitteilung Nr. 20210310_2 vom 10. März 2021 darauf hin, dass eine Meldung zu erfolgen hat, wenn bei der vorzunehmenden Überprüfung eine „Kompromittierung der Systeme festgestellt“ wird.

Mögliche Risiken einer nicht erforderlichen Meldung

Im Zusammenhang mit der Proxylogon-Sicherheitslücke wurde von rechtsberatender Seite durchaus Kritik an den als uneinheitlich und teilweise zu extensiv empfundenen Aussagen zur Meldepflicht geäußert, allerdings vielfach empfohlen, u. a. aufgrund der (vermeintlichen) Schutzwirkung einer Meldung nach §§ 42 Abs. 4, 43 Abs. 4 BDSG „im Zweifel“ eine Meldung vorzunehmen.

Ob diese Empfehlung tatsächlich richtig ist, kann zumindest in rechtlicher Sicht aus guten Gründen bezweifelt werden. Die Zweifel gelten im Übrigen nicht nur im Hinblick auf die Proxylogon-Sicherheitslücke, sondern ganz allgemein im Hinblick auf die Empfehlung, „im Zweifel“ zu melden. Zunächst ist richtig, dass §§ 42 Abs. 4, 43 Abs. 4 BDSG eine Schutzwirkung zugunsten des Meldepflichtigen bzw. des Benachrichtigenden entfalten, wobei es hier wiederum auf Details ankommt. § 42 BDSG betrifft das Straf- und § 43 BDSG das Ordnungswidrigkeitenverfahren, inhaltlich sind beide Normen ansonsten identisch.

Nach § 43 Abs. 4 BDSG (der teilweise als europarechtswidrig angesehen wird, siehe dazu Spittka, DSB 2019, 217 ff.) darf eine Meldung nach Art. 33 DSGVO im Ordnungswidrigkeitenverfahren „gegen den Meldepflichtigen oder Benachrichtigenden […] nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden“. Daraus zu schließen, dass eine Meldung nach Art. 33 Abs. 1 Satz 1 DSGVO zur Folge hat, dass im Zusammenhang mit dem gemeldeten Sachverhalt keine Sanktion erfolgen kann, geht leider mehrfach fehl. Zum einen ist zu berücksichtigen, dass der Schutz der §§ 42 Abs. 4, 43 Abs. 4 BDSG nur dann besteht, wenn es sich um eine Meldung nach Art. 33 DSGVO handelt. Die Meldepflicht muss also bestehen. Zum anderen gilt der Schutz auch nur im Hinblick auf meldepflichtige Tatsachen. Wird also „zu viel“ gemeldet oder erfolgt eine Meldung, zu der ein Verantwortlicher gar nicht verpflichtet war, besteht im Hinblick auf den nicht erforderlichen Teil der Meldung keine Schutzwirkung, so dass die Meldung selbst Auslöser für Sanktionen werden kann.

Wird beispielsweise ein rein materieller datenschutzrechtlicher Verstoß gemeldet, wie eine (im jeweils konkreten Fall) unzulässige Verarbeitung von Kundendaten im

Rahmen einer Direktmarketing-Aktion, besteht keine Schutzwirkung, da dies regelmäßig nicht mit einer Verletzung des Schutzes personenbezogener Daten i. S. v. Art. 4 Nr. 12 DSGVO einhergeht. Die Definition der „Verletzung des Schutzes personenbezogener Daten" in Art. 4 Nr. 12 DSGVO setzt nämlich ausdrücklich die „Verletzung der Sicherheit" voraus, die z.B. bei der unzulässigen Verwendung eines Nutzerprofils für Direktmarketing nicht vorliegen muss und auch häufig nicht vorliegen wird. Dasselbe gilt, wenn zwar eine solche Verletzung des Schutzes personenbezogener Daten vorliegt (z. B. durch den Verlust personenbezogener Daten durch die versehentliche Unbrauchbarmachung eines Datenträgers), dies aber voraussichtlich nicht zu einem Risiko für die Betroffenen führt.

Es mag zwar auf den ersten Blick merkwürdig erscheinen, dass eine überobligatorische Meldung aus Sicht des Gesetzgebers keine Schutzwirkung entfalten soll, im Kern ist dies jedoch nachvollziehbar. Die DSGVO sieht eine solche Schutzwirkung nicht vor. Der nationale Gesetzgeber hat hier jedoch das Prinzip „nemo tenetur se ipsum accusare", wonach sich niemand selbst belasten muss, angewendet (vgl. Spittka, DSB 2019, 217, 217 ff.). Nach diesem Prinzip muss die Erfüllung einer zwingenden Auskunftspflicht einem strafrechtlichen Verwertungsverbot unterliegen. Würde man jede Meldung zum Gegenstand eines Verwertungsverbots machen, hätte dies überspitzt ausgedrückt zur Folge, dass ein Verantwortlicher Datenschutzverstöße nur melden müsste, um einer Sanktion zu entgehen. Ein solcher Freibrief ist mit §§ 42 Abs. 4, 43 Abs. 4 BDSG erkennbar nicht bezweckt.

Allgemeine Empfehlungen im Hinblick auf Meldung nach Art. 33 Abs. 1 Satz 1 DSGVO

Wie dargestellt dürfte die Empfehlung, „im Zweifel" eine Meldung nach Art. 33 Abs. 1 Satz 1 DSGVO vorzunehmen, unzutreffend sein. Vielmehr ist zu empfehlen, zunächst zu prüfen, ob eine Meldung offensichtlich zu erfolgen hat. Bei „Zweifeln" ist eine Rechtsberatung einzuholen.

Sofern die für das eigene Unternehmen zuständige Datenschutzbehörde klare Aussagen zur Meldepflicht gemacht hat, ist es selbstverständlich sinnvoll, zu prüfen, ob die Datenschutzbehörde eine solche Meldepflicht annimmt. Nimmt die zuständige Datenschutzbehörde keine Meldepflicht an, sollte eine Meldung aus rechtlicher Sicht unterbleiben (auch wenn man einwenden mag, dass Datenschutzbehörden in der Praxis „wohlwollend" auf Meldungen reagieren). Deutlich wird dies am Beispiel einer Meldung im Zusammenhang mit der Proxylogon-Sicherheitslücke, die nur deswegen erfolgt, weil die zur Verfügung gestellten Sicherheitsupdates verspätet eingespielt wurden und eine Kompromittierung nicht ausgeschlossen werden kann. Erfolgt eine Meldung gegenüber einer Datenschutzbehörde, die keine Meldepflicht annimmt, besteht keine Schutzwirkung nach §§ 42 Abs. 4, 43 Abs. 4 BDSG. Gleichzeitig räumt der meldende Verantwortliche mit an Sicherheit grenzender Wahrscheinlichkeit einen schuldhaften Verstoß gegen die Pflichten nach Art. 32 DSGVO ein. In der Regel kann kaum begründet werden, warum nicht auf die seit dem 3. März 2021 bekannte Bedrohungslage reagiert wurde.

Nimmt die zuständige Datenschutzbehörde eine Meldepflicht an, ist zu überlegen, ob auch bei eigener gegenteiliger Ansicht eine Meldung opportun ist. Zwar besteht in dem Fall, dass die Datenschutzbehörde die Meldepflicht zu Unrecht annimmt, ebenfalls keine Schutzwirkung nach §§ 42 Abs. 4, 43 Abs. 4 BDSG, allerdings ist anzunehmen, dass sich die Datenschutzbehörden nicht in Widerspruch zu ihrer eigenen Auffassung setzen und die Meldung zum Anlass für Sanktionen nehmen. Zu berücksichtigen ist allerdings, dass die zuständige Staatsanwaltschaft im Fall einer möglichen Strafbarkeit nach § 42 BDSG nicht an die Wertung der Datenschutzbehörde gebunden ist und daher eine Meldung, sofern eine Straftat im Raum steht, nur unter Einholung entsprechender Rechtsberatung in Betracht gezogen werden sollte.

Wann sind „Verletzungen der Sicherheit" zu melden?

Aufgrund der uneinheitlichen Auffassungen der Aufsichtsbehörden bei der Proxylogon-Sicherheitslücke werden nachfolgend die verschiedenen Kategorien dargestellt und bewertet.

Eindeutige Fälle

Eindeutig sind die Fälle, in denen nachweislich ein Abfluss personenbezogener Daten von einem IT-System stattgefunden hat. Dann gilt, dass eine Meldung nach Art. 33 Abs. 1 Satz 1 DSGVO zu machen ist, „es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt". Nach Art. 33 Abs. 5 DSGVO ist dann intern zu dokumentieren, warum ein solches Risiko nicht angenommen wird (diese Dokumentation wird häufig vergessen).

Genauso eindeutig ist der Fall, in dem bereits eine Kompromittierung des IT-Systems trotz bestehender Sicherheitslücke ausgeschlossen werden kann, oder wenn trotz möglicher oder tatsächlicher Kompromittierung ausgeschlossen werden kann, dass eine Kenntnisnahme oder Änderung der in dem System gespeicherten personenbezogenen Daten stattgefunden hat. Je nach Sachverhalt liegt dann schon keine notwendige Verletzung des Schutzes personenbezogener Daten nach Art. 4 Nr. 12 DSGVO vor, oder aber die Verletzung führt nicht zu einem Risiko für die Betroffenen. Dann ist es auch irrelevant, ob und wie lange eine Sicherheitslücke bestanden hat.

Problematische Fälle

Problematischer sind jedoch (nicht abschließend) Fälle, in denen zwar eine Kompromittierung nicht ausgeschlossen, aber auch nicht nachgewiesen werden kann. Am Beispiel der Proxylogon-Sicherheitslücke wird z. B. – wie oben zitiert – seitens der LfD Niedersachsen davon ausgegangen, dass bereits das verspätete Einspielen der Sicherheitsupdates eine Meldepflicht auslöse. Dies beruht wohl auf dem Umstand, dass das BSI erklärte, dass von einer Kompromittierung auszugehen sei, wenn die Updates nicht bis zum 5. März 2021 erfolgt seien. Dabei wird eine doppelte Vermutung (ohne Nachweis) aufgestellt, nämlich dass als notwendiger Zwischenschritt eine Kompromittierung stattgefunden hat und dass diese auch dahingehend ausgenutzt wurde, dass personenbezogene Daten unbefugt zur Kenntnis Dritter gelangt sind oder aber in ihrer Integrität beeinträchtigt wurden.

Bei dieser Anwendung von Art. 33 Abs. 1 Satz 1 DSGVO und Art. 4 Nr. 12 DSGVO wird jedoch übersehen, dass zunächst einmal zwei verschiedene „Pflichtenprogramme" ablaufen. Unbestritten verpflichtet Art. 32 DSGVO dazu, umgehend und fortlaufend zu prüfen, inwieweit die Sicherheit der Verarbeitung beeinträchtigt ist und Maßnahmen zur Wiederherstellung der Sicherheit der Verarbeitung zu treffen. Das Unterlassen der Prüfung und/oder entsprechender Maßnahmen an sich stellt bereits einen Verstoß gegen Art. 32 DSGVO dar. Gleichzeitig ist ein solcher Fall Anlass zur Prüfung, ob eine Meldepflicht nach Art. 33 Abs. 1 Satz 1 DSGVO besteht (sowie natürlich auch nach Art. 34 DSGVO, aber dies ist nachgelagert). Maßstab einer solchen Prüfung ist allein das Gesetz, welches zunächst eine Verletzung des Schutzes personenbezogener Daten nach Art. 4 Nr. 12 DSGVO verlangt. Die Definition spricht von einer „Verletzung der Sicherheit", welche in der hier relevanten Kategorie der unberechtigten Kenntnisnahme „zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten" führen muss.

Zweifelsohne stellt ein nicht gepatchtes System bei einer gravierenden Sicherheitslücke wie Proxylogon eine Verletzung der Sicherheit dar (und zwar seit Beginn des Betriebs des entsprechenden Exchange Servers). Die Verletzung der Sicherheit muss jedoch darüber hinaus auch zu einem „Erfolg" in Form der unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten führen. Die reine Möglichkeit dürfte hierfür nicht reichen, da dies die Definition nicht hergibt. In diesem Zusammenhang wird man sicherlich nicht absolute Gewissheit einer unbefugten Kenntnisnahme verlangen können. Die gesetzliche Definition wird jedoch überstrapaziert, wenn man aus einem tatbestandlich geforderten Erfolg mit der Anforderung „es sei denn, die Kenntnisnahme kann ausgeschlossen werden" dem Verantwortlichen auferlegt, nachzuweisen, dass eine Kenntnisnahme nicht erfolgt ist.

Dem kann auch nicht das Beispiel des verlorenen gegangenen USB-Sticks oder sonstiger Datenträger entgegengehalten werden, wo sicherlich eine Meldepflicht angenommen werden kann. Wenn z. B. der Sportdirektor eines Fußball-Bundesligisten einen Rucksack mit Gehaltslisten und Scouting-Reports in der Bahn liegen lässt oder dieser gestohlen wird und später in einem Park wieder auftaucht, wird sich der Verantwortliche (der Bundesligist) kaum darauf verlassen können, dass eine Kenntnisnahme der (sensiblen) personenbezogenen Daten nicht erfolgt und in dieser Hoffnung eine Meldung unterlassen. Die Frage, ob Dritte Kenntnis nehmen, liegt nämlich weder im Einflussbereich des Verantwortlichen, noch kann er dies prüfen.

Wenn aber unter Ausschöpfung angemessener Mittel ein „Datenabfluss" zwar nicht ausgeschlossen werden kann, hierfür aber auch keine Anhaltspunkte bestehen (diese bestehen beim abhanden gekommenen Rucksack), sollte dies entgegen der Auffassung mancher Datenschutzbehörde keine Meldepflicht auslösen. Gleichwohl besteht selbstverständlich die Pflicht, eine mögliche Kompromittierung fortlaufend zu prüfen und bei deren Vorliegen eine Meldung ggf. zu einem späteren Zeitpunkt vorzunehmen.

Fazit

Im Hinblick auf Meldepflichten nach Art. 33 Abs. 1 Satz 1 DSGVO nehmen Datenschutzbehörden gelegentlich eine (zu) extensive Auslegung vor. Tritt eine Verletzung der Sicherheit (zumeist IT-Sicherheit) ein, sind im Hinblick auf eine mögliche Meldung folgende Grundsätze zu beachten:

- Zunächst ist am Maßstab von Art. 33 Abs. 1 Satz 1 DSGVO und Art. 4 Nr. 12 DSGVO zu prüfen, ob eine Meldepflicht besteht; die Empfehlung, „im Zweifel" zu melden, überzeugt aus rechtlicher Sicht nicht.
- Bestehen Zweifel und hat die für das eigene Unternehmen zuständige Datenschutzbehörde Aussagen zur Meldepflicht im konkreten Fall gemacht, sollte eine Meldung nur dann erfolgen, wenn die Datenschutzbehörde eine Meldepflicht annimmt; steht eine mögliche Strafbarkeit nach § 42 BDSG im Raum, sollte zwingend eine entsprechende Rechtsberatung eingeholt werden.
- Erfolgt eine Meldung, hat sich diese auf die in Art. 33 Abs. 3 DSGVO aufgelisteten erforderlichen Informationen zu beschränken.

Autor: **Gerhard Deiters ist Rechtsanwalt und Partner bei BHO Legal in Köln. Er ist im IT- und Datenschutzrecht sowie auf die Bereiche Luft- und Weltraum spezialisiert. Er ist zudem bei der BHO Consulting GmbH als externer Datenschutzbeauftragter tätig.**