AOK VERLAG

Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

Ausgabe April 2017 | Seite 1

www.aok-verlag.info/ds-im-blick

INHALT

Datenschutz-Folgenabschätzung

Ab Mai 2018 gilt die EU-Datenschutz-Grundverordnung (DS-GVO). Neben vielen bekannten Regelungen bringt diese auch verschiedene Neuerungen mit sich. Eine dieser „Neuerungen" ist die sogenannte Datenschutz-Folgenabschätzung. Diese ist Gegenstand des nachfolgenden Beitrags.

Dr. Sebastian Ertel

Rechtliche Grundlage

Geregelt ist die Datenschutz-Folgenabschätzung (DSFA) in Art. 35 DS-GVO:

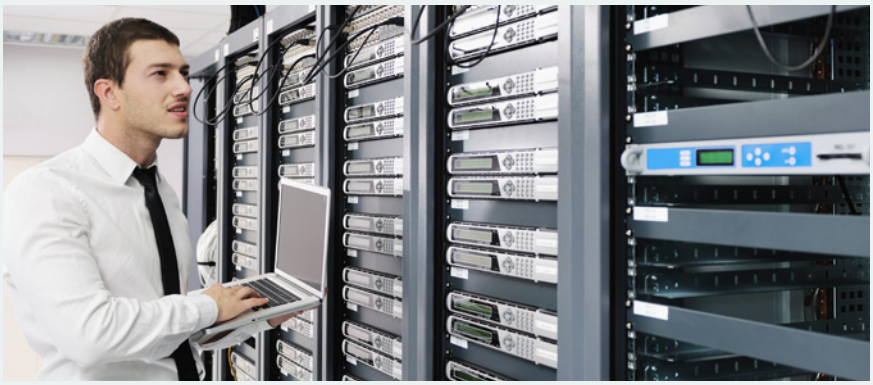
„Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden."

Flankiert wird Art. 35 durch verschiedene Erwägungsgründe zur DS-GVO. Durch die Erwägungsgründe werden die Ziele, die mit der Formulierung der Artikel der DS-GVO verfolgt wurden, dargelegt. Die Erwägungsgründe dienen daher insbesondere der Auslegung der DS-GVO.

Auffällig ist, dass die DSFA nicht durch den Datenschutzbeauftragten (DSB) durchzuführen ist, sondern durch den Verantwortlichen (für die Datenverarbeitung). Gleichwohl wird der DSB in den Prozess eingebunden.

Dieser steht dem Verantwortlichen beratend zur Seite.

Aus Art. 35 Abs. 4 und 5 DS-GVO ergibt sich, dass die Aufsichtsbehörde eine Übersicht der Verfahren, die die Durchführung einer DSFA erfordern, erstellt und veröffentlicht. Zudem kann eine zweite Liste für die Verfahren erstellt werden, für die es keiner DSFA bedarf.



Vorabkontrolle 2.0?

Blickt man in das Bundesdatenschutzgesetz (BDSG), stößt man zwangsläufig auf § 4 Abs. 5 BDSG, der die Vornahme einer Vorabkontrolle regelt, soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen. Insoweit ist die Frage berechtigt, ob die DSFA lediglich eine Überarbeitung der Vorabkontrolle ist. Das Bayerische Landesamt für Datenschutzaufsicht erteilt diesem Verständnis eine klare Absage. Die Vorabkontrolle unterliegt keinen festen Prozessen, während die DSFA eine systematische Vorgehensweise und differenzierte Dokumentation erfordert. Bereits aus diesem Grund sind, trotz unstreitiger Schnittmengen, beide Verfahren als selbständige Instrumente des Datenschutzes anzusehen.

Ansatzpunkt der DSFA

Eine DSFA ist nur erforderlich, sofern der Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen immanent ist.

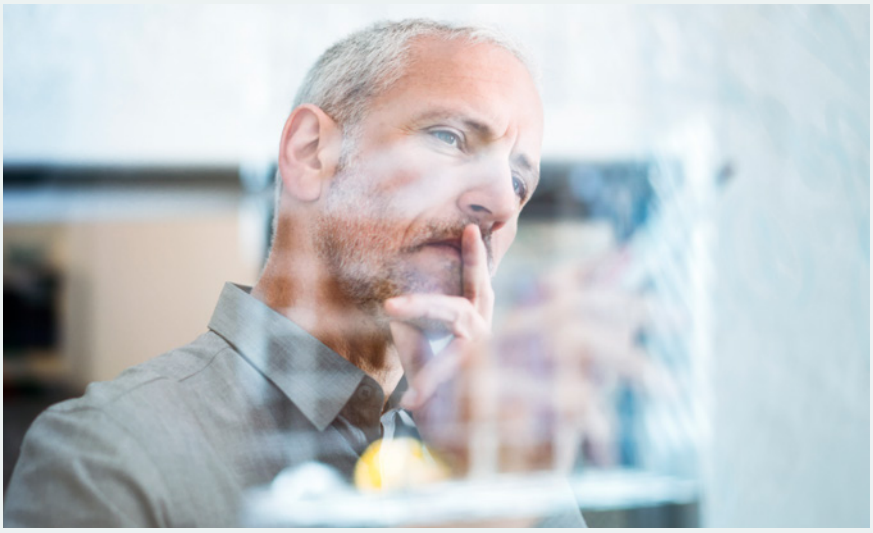
Dies wird per se bei umfangreichen Verarbeitungsvorgängen angenommen, die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten, eine große Zahl von Personen betreffen könnten und beispielsweise aufgrund ihrer Sensibilität wahrscheinlich ein hohes Risiko mit sich bringen (Erwägungsgrund 91). Die DS-GVO definiert in Art. 35 Abs. 3 Konstellationen, in denen eine DSFA zwingend ist.

- bei systematischer und umfassender Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlicher Weise erheblich beeinträchtigen;
- bei umfangreicher Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten;
- bei systematischer weiträumiger Überwachung öffentlich zugänglicher Bereiche.

Die Rechte und Freiheiten des Betroffenen sind nach Erwägungsgrund 75 dann gefährdet, wenn die Datenverarbeitung geeignet ist,

- eine Diskriminierung,
- einen Identitätsdiebstahl oder -betrug,
- einen finanziellen Verlust,
- eine Rufschädigung,
- den Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten,
- das unbefugte Aufhebung der Pseudonymisierung oder
- andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile

zu verursachen.



Im Vorfeld ist daher eine Risikoanalyse vorzunehmen, die gemäß Erwägungsgrund 90 die spezifische Eintrittswahrscheinlichkeit und die Schwere des Risikos anhand der Kriterien

- Art,
- Umfang,
- Umstände und
- Zwecke der Verarbeitung und Ursachen des Risikos

bestimmt. Im Rahmen der Risikoanalyse genießt die Schwere eines möglichen Schadens vorrangige Priorität. Der Eintrittswahrscheinlichkeit kommt nur eine untergeordnete Berücksichtigung zu.

Durchführung der DSFA

Nach der Risikobewertung erfolgt die eigentliche Durchführung der DSFA. Diese ist durch Art. 35 Abs. 7 DS-GVO klar definiert (im Gegensatz zur Vorabkontrolle nach § 4 d Abs. 5 und 6 BDSG).

Zunächst ist das geplante Verfahren mit sämtlichen Datenerhebungen und -verarbeitungen detailliert zu beschreiben. In diesem Zusammenhang müssen auch die Zwecke, die mit der Datenverarbeitung verfolgt werden, klar herausgearbeitet werden. Dies ist insoweit erforderlich, um anschließend die entsprechenden Rechtsgrundlagen und deren Voraussetzungen zu definieren und zu prüfen.

Hieran schließt sich die Bewertung der Notwendigkeit der Datenverarbeitung an. Hierbei spielt die Verhältnismäßigkeit und insoweit die Prüfung weniger eingriffsintensiver Alternativen eine maßgebliche Rolle.

Im Weiteren sind die in der Vorprüfung festgestellten Risiken für die Freiheiten und Rechte der von der Datenverarbeitung Betroffenen zu bewerten.

Letztlich bedarf es einer detaillierten Beschreibung der Maßnahmen und Vorkehrungen, durch die der Schutz der Betroffenen gewährleistet wird.

Ergebnisse der DSFA

Als Ergebnis einer DSFA sind vier Varianten denkbar.

- Das Verfahren ist datenschutzrechtlich zulässig und kann bedenkenlos eingesetzt werden.
- Das Verfahren ist in der derzeitigen Form datenschutzwidrig. Die Datenschutzwidrigkeit kann aber durch entsprechende Maßnahmen beseitigt werden.
- Das Verfahren ist datenschutzwidrig und die Punkte, die zur Datenschutzwidrigkeit führen, sind nicht zu beseitigen.
- Die DSFA kann aber auch zu einem nicht eindeutigen Ergebnis führen.

Hier greift die Regelung des Art. 36 Abs. 1 DS-GVO. Danach hat der Verantwortliche (nicht der Datenschutzbeauftragte, wie bei der Vorabkontrolle – § 4d Abs. 6 S. 3 BDSG) vor der Verarbeitung die Aufsichtsbehörde zu konsultieren, wenn aus der DSFA hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft. In diesem

Fall muss der Verantwortliche der Aufsichtsbehörde umfassende, in Art. 36 Abs. 3 DS-GVO aufgeführte Informationen zur Verfügung stellen, damit diese innerhalb einer Regelfrist von acht Wochen über die Zulässigkeit des Verfahrens entscheidet (Art. 36 Abs. 2 DS-GVO). Die Frist kann in bestimmten Fällen um sechs Wochen verlängert werden.

Nichtdurchführung der DSFA

Führt der Verantwortliche die DSFA nicht durch oder konsultiert er bei nicht eindeutigen Ergebnissen nicht die Aufsichtsbehörde, erfüllt er hierdurch den Bußgeldtatbestand des Art. 83 Abs. 4a DS-GVO, der ein Bußgeld von bis zu 10 Millionen Euro oder 2 % des gesamten weltweiten Jahresumsatzes nach sich ziehen kann.

Kurznotiz:

Schließkonzept

Innerhalb einer Gesundheitseinrichtung gibt es eine Vielzahl an Funktionsräumen, die im Idealfall alle abschließbar sind. Zum Teil ermöglichen insbesondere Reha-Einrichtungen ihren stationär aufgenommenen Patienten, die Zimmer abzuschließen. Bei der Vergabe entsprechender Zutrittsrechte zu Funktionsräumen und Patientenzimmern ist die konkrete Tätigkeit des jeweiligen Mitarbeiters maßgeblich. So darf dieser ausschließlich die Gebäude/Bereiche/Räume betreten, die er für die Erfüllung seiner arbeitsvertraglichen Aufgaben zwangsnotwendig betreten muss. Zu sämtlichen anderen Gebäuden/Bereichen/Räumen sind ihm die Zutrittsberechtigungen zu verwehren.

Es ist insoweit erforderlich, vor der Ausgabe der Schlüssel/Karten/Transponder im Rahmen eines Zutrittskonzepts die Tätigkeiten der verschiedenen Beschäftigtengruppen zu erfassen und anhand dessen die jeweiligen Zutrittsrechte zu definieren. Hierdurch wird zudem gewährleistet, dass die verantwortliche Stelle ihren Kontroll- und Nachweispflichten hinsichtlich des Datenschutzes und der Datensicherheit nachkommt. Jede Vergabe von Zutrittsrechten (z. B. in Form von Schlüsseln oder Berechtigungen) sollte zudem dokumentiert werden, um bei einem Wechsel des Aufgabenbereichs des Mitarbeiters bzw. beim Verlassen der Einrichtung die Zutrittsrechte auch wieder entziehen zu können.

Verzeichnis der Verarbeitungstätigkeiten nach der DS-GVO – was ändert sich?

Ab dem 25. Mai 2018 gilt die DS-GVO. Einrichtungen des Gesundheitswesens haben daher noch gut ein Jahr Zeit, sich auf die neue Rechtslage vorzubereiten. Diese sollten allerdings jetzt schon damit beginnen, ihr bestehendes Verfahrensverzeichnis an die Anforderungen der DS-GVO anzupassen. Dieser Beitrag gibt eine erste Orientierungshilfe, was dabei zu beachten ist und an welchen Stellen sich das neue Verzeichnis vom bisherigen Verfahrensverzeichnis unterscheidet.

Sven Venzke-Caprarese

Der Name

Zunächst ändert sich der Name des Verfahrensverzeichnisses. Nach Art. 30 DS-GVO wird aus dem „Verfahrensverzeichnis“ das „Verzeichnis von Verarbeitungstätigkeiten“.

Die Voraussetzungen der Pflicht zum Führen des Verzeichnisses

Auch die Voraussetzungen, unter denen ein Verzeichnis der Verarbeitungstätigkeiten zu führen ist, ändern sich. Nach Art. 30 Abs. 5 DS-GVO müssen Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, grundsätzlich kein solches Verzeichnis führen. Etwas anderes gilt aber dann, wenn alternativ einer der folgenden Punkte vorliegt:

- die von der Einrichtung vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen;
- die Verarbeitung erfolgt nicht nur gelegentlich;
- es werden besondere Datenkategorien (z. B. Gesundheitsdaten) verarbeitet.

Insbesondere der letztgenannte Punkt liegt bei Gesundheitseinrichtungen immer vor, weshalb diese auch in Zukunft ein entsprechendes Verzeichnis vorhalten müssen.

Darüber hinaus macht die Rechenschaftspflicht nach Art. 5 DS-GVO das Verzeichnis von Verarbeitungstätigkeiten zum unverzichtbaren und zentralen Bestandteil eines jeden Datenschutzmanagements. Denn ohne ein Verzeichnis über die Verarbeitungstätigkeiten einer Einrichtung ist eine geordnete Dokumentation und organisierte Steuerung von datenschutzrelevanten Prozessen in der Praxis kaum möglich.

Kein Einsichtsrecht für Jedermann

Bislang mussten Datenschutzbeauftragte das Verfahrensverzeichnis gem. § 4g Abs. 2 S. 2 BDSG auf Antrag gegenüber jedermann in geeigneter Weise verfügbar machen. Dies ändert sich mit Wirksamwerden der DS-GVO grundlegend.

Nach Art 30 Abs. 4 DS-GVO wird das Verzeichnis der Verarbeitungstätigkeiten nur noch durch den Verantwortlichen auf Anfrage der Aufsichtsbehörde dieser zur Verfügung gestellt.

Auch wenn das Verzeichnis der Verarbeitungstätigkeiten damit auf den

ersten Blick erheblich an Bedeutung verliert, ist es dennoch von zentraler Bedeutung. Denn wie bereits dargestellt, kann das Verzeichnis der Verarbeitungstätigkeiten als Grundstein des Datenschutzmanagements und der Datenschutzorganisation innerhalb der Einrichtung genutzt werden.

Inhalte unterscheiden sich auf den ersten Blick nur marginal

Die Inhalte des Verzeichnisses der Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DS-GVO und die Inhalte des Verfahrensverzeichnisses nach § 4e BDSG unterscheiden sich nur marginal. Legt man den Wortlaut beider Rechtsvorschriften nebeneinander und vergleicht die Inhalte, zeigen sich nur an zwei Stellen Informationen, die im Verzeichnis der Verarbeitungstätigkeiten aufgenommen werden müssen, die das Verfahrensverzeichnis bislang nicht vorschreibt.

§ 4e BDSG		Art. 30 Abs. 1 DS-GVO	
Nr. 1	Name oder Firma der verantwortlichen Stelle	**lit. a**	Namen
Nr. 3	Anschrift der verantwortlichen Stelle		Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen
Nr. 2	Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen		Kontaktdaten des Vertreters des Verantwortlichen
Diese Anforderung ist neu und muss aufgenommen werden.		**lit. a**	sowie eines etwaigen Datenschutzbeauftragten
Nr. 4	Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung	**lit. b**	Zwecke der Verarbeitung
Nr. 5	Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien	**lit. c**	Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
Nr. 6	Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	**lit. d**	Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen
Nr. 7	Regelfristen für die Löschung der Daten	**lit. f**	wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
Nr. 8	geplante Datenübermittlung in Drittstaaten	**lit. e**	gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation
Diese Anforderung ist neu und muss aufgenommen werden.		**lit. e**	einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien
Nr. 9	allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind	**lit. g**	wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1

Technische und organisatorische Maßnahmen

Eine Änderung für das Verzeichnis der Verarbeitungstätigkeiten ergibt sich jedoch in der Darstellung der technischen und organisatorischen Maßnahmen. Nach § 4e Nr. 9 BDSG mussten im Verfahrensverzeichnis bislang die angemessenen Maßnahmen nach § 9 BDSG zur Gewährleistung der Sicherheit der Verarbeitung beschrieben werden. Über die Anlage zu § 9 S. 1 BDSG ließen sich die Maßnahmen bisher wie folgt kategorisieren:

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Zwecktrennungsgebot

Die technischen und organisatorischen Maßnahmen der DS-GVO lassen sich nach Art. 32 Abs. 1 DS-GVO hingegen in diesen Kategorien darstellen:

- Pseudonymisierung und Verschlüsselung
- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Belastbarkeit
- Wiederherstellbarkeit
- Überprüfung, Bewertung und Evaluierung

Zwar werden sich die meisten Kategorien technischer und organisatorischer Maßnahmen des BDSG den Maßnahmekategorien der DS-GVO zuordnen lassen. Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen war bislang durch das BDSG in dieser Ausdrücklichkeit jedoch nicht vorgeschrieben.

Es kann insofern sinnvoll sein, das Verzeichnis der Verarbeitungstätigkeiten um eine Planung interner Audits zu erweitern, in der kurz auf vergangene Audits hingewiesen wird und in der Termine künftiger Audits geplant werden.

Der Begriff „Verarbeitungstätigkeiten“ kann zu erheblichen Veränderungen führen

Darüber hinaus besteht ein weiterer Unterschied des Verfahrensverzeichnisses nach BDSG und des Verzeichnisses der Verarbeitungstätigkeiten nach DS-GVO. Denn nach § 4e BDSG waren in das Verfahrensverzeichnis lediglich „Verfahren automatisierter Verarbeitungen“ aufzunehmen. Nach Art. 30 DS-GVO sind hingegen alle „Verarbeitungstätigkeiten“ aufzunehmen. Nach Art. 4 Abs. 2 DS-GVO ist unter „Verarbeitung“ jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten zu verstehen.

Ob und ggf. wie sich dieser Unterschied in der Praxis auswirken wird, ist derzeit noch unklar. Es ist jedoch denkbar, dass in das Verzeichnis der Verarbeitungstätigkeiten künftig auch Dateisysteme i.S.d. Art. 4 Nr. 6 DS-GVO aufgenommen werden müssen. In der Praxis beträfe dies vor allem die Aufnahme gleichartig aufgebauter Papierakten, für welche dann ebenfalls die Angaben des Art. 30 Abs. 1 DS-GVO dargestellt werden müssten.

Auftragsverarbeiter in der Pflicht

Grundlegend neu ist die Verpflichtung aus Art. 30 Abs. 2 DS-GVO, nach der auch Auftragsverarbeiter ein eigenes Verzeichnis der Verarbeitungstätigkeiten zu führen haben. Das Verzeichnis unterscheidet sich somit von dem Verzeichnis, welches der Verantwortliche zu führen hat. Welche Punkte ein Auftragsverarbeiter in sein Verzeichnis aufzunehmen hat, ergibt sich aus Art. 30 Abs. 2 DS-GVO.

Sanktionsmöglichkeiten

Gemäß Art. 83 Abs. 4 DS-GVO kann ein Verstoß gegen die Pflicht zur Führung bzw. zur Vorlage eines Verzeichnisses gegenüber der Aufsichtsbehörde nach Art. 30 Abs. 1 DS-GVO Geldbußen von bis zu 10.000.000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs zur Folge haben. Im Gegensatz dazu war ein fehlendes Verfahrensverzeichnis nach dem BDSG nicht bußgeldbewehrt (da sich in § 43 BDSG kein entsprechender Bußgeldtatbestand findet).

Datenschutz im Gesundheitswesen

Grundlagenwissen – Praxislösungen – Entscheidungshilfen

2 Ordner mit Register im Format DIN A5,
ca. 1.500 Seiten Inhalt
ISBN: 978-3-553-43000-5
Preis 179.- inkl. MwSt.

Uneingeschränkter Online-Zugriff auf alle Arbeitshilfen inkl. 3-4 kostenpflichtige Nachtragslieferungen pro Jahr zum Preis von jeweils 79,90 Euro inkl. MwSt. und versandkostenfreier Zusendung im Inland.

© AOK-Verlag GmbH | Lilienthalstraße 1-3 | 53424 Remagen | Tel 02642 931-333 | Fax 02642 931-215 | Mail fachinfo@aok-verlag.de | Web: http://www.aok-verlag.info | Herausgeber: AOK-Verlag GmbH, Remagen | Geschäftsführung: Otto Gmeiner | Redaktion: Prof. Dr. Benedikt Buchner, Dr. Sebastian Ertel, Sven Venzke-Caprarese | Der Inhalt des vorliegenden Newsletters ist mit größter Sorgfalt zusammengestellt worden. Eine Haftung für die Angaben übernimmt der Verlag jedoch nicht. Bildnachweise: www.istock.com