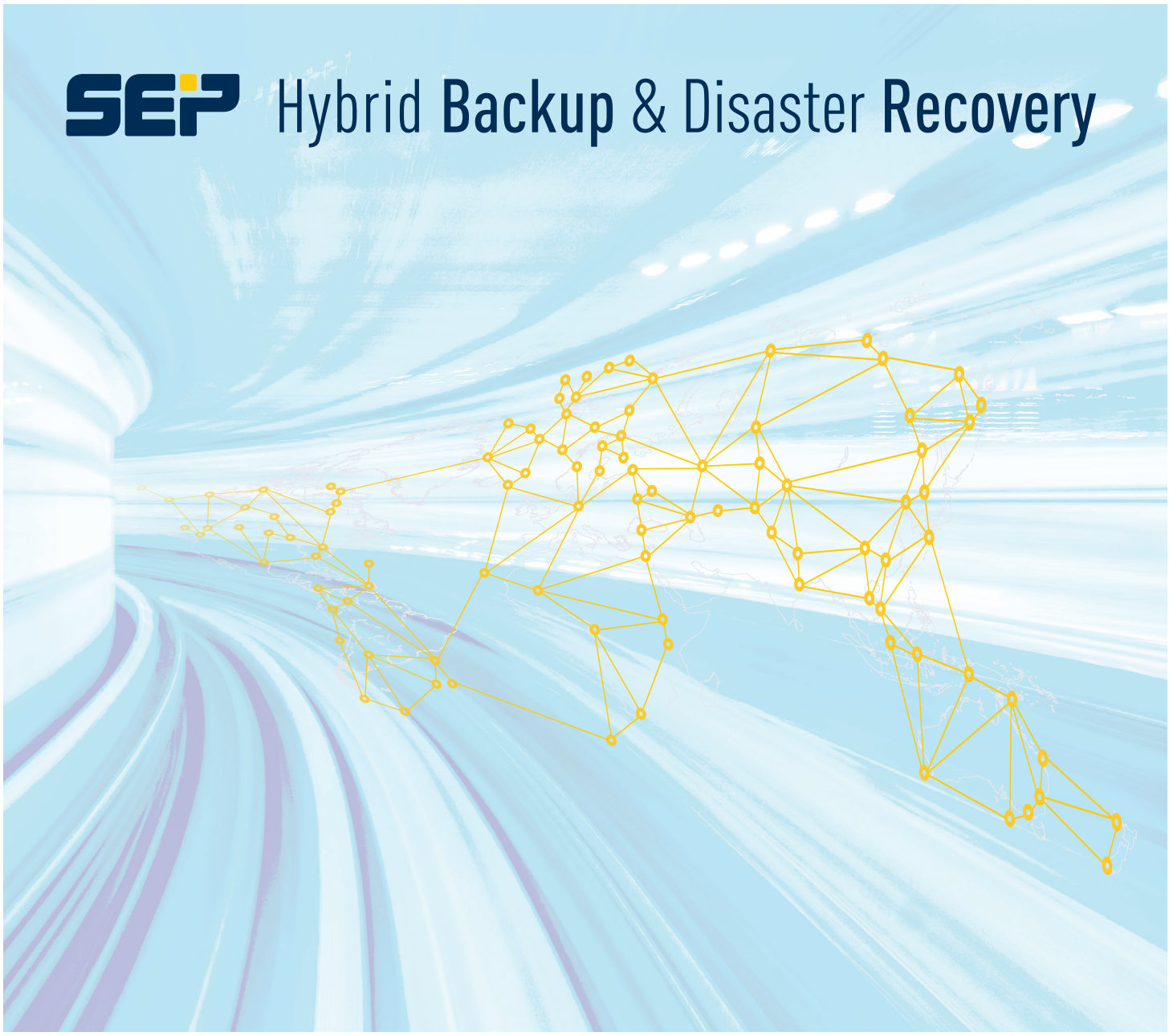

Datenschutzgrundverordnung, NIS-Richtlinie der EU & das IT-Sicherheitsgesetz

Ein neues, einheitliches Datensicherheits- / Datenschutzrecht für Europa

Von Rechtsanwalt und Fachanwalt für IT-Recht Dr. Jens Bücking

Inhaltsverzeichnis

Einführung 3

1.„Unentrinnbar"(1) – der weite geographische Anwendungsbereich der EU-DSGVO .. 4

2.„Unentrinnbar"(2) – die extensive Auslegung des Anwendungsbereichs „personenbezogene Daten" im Sinne der EU-DSGVO 4

3. Die wichtigsten Neuerungen 5

4. Auftragsverarbeitung: Neue Haftungskonzepte bei Cloud & Co. 5

5. Datenschutz-Folgeabschätzung 6

6. Datenschutzkonzept und technisch-organisatorische Datensicherheitsmaßnahmen 6

7. Datenschutz durch Technik 6

8. Benachrichtigungspflichten bei Verstößen 7

9. Betriebliche und behördliche Datenschutzbeauftragte 7

10. Geldbußen, Schadensersatz, Verarbeitungsstopp: Verschärfte Sanktionsmittel 7

11. Auswirkungen auf Industrie 4.0 und Big Data 8

12. IT-Sicherheitsgesetzgebung in Deutschland und Europa 9

Rechtssicherheit durch technische Sicherheit Lösungskonzepte von SEP 13

Die globale Lösung - Made in Germany 14

Abkürzungsverzeichnis 15

* Der Autor ist Rechtsanwalt und Fachanwalt für IT¬-Recht. Er ist darüber hinaus Gründungspartner der Rechtsanwaltskanzlei e/s/b Rechtsanwälte (http://www.kanzlei.de) sowie zugleich Fachbuchautor im IT¬-Recht und Lehrbeauftragter an der Hochschule für Technik in Stuttgart und als associate Professor an der E.N.U. in Kerkrade, Niederlande tätig.

** Disclaimer: Dieses Dokument stellt eine generelle rechtliche Bewertung dar. Es ersetzt nicht die verbindliche Rechtsauskunft durch einen spezialisierten Anwalt. Bitte haben Sie Verständnis, dass trotz größtmöglicher Sorgfalt bei der Erstellung eine Garantie oder Haftung für die inhaltliche Richtigkeit, Aktualität und individuelle Brauchbarkeit nicht übernommen wird.

Einführung

Die EU-Datenschutz-Grundverordnung (VO) steht seit dem 25.05.2016 in Kraft und wird nach einer zweijährigen Übergangsfrist geltendes Recht. Die VO ersetzt in den EU-Mitgliedstaaten die bislang geltende EU-Datenschutzrichtlinie aus dem Jahre 1995 und die in deren Umsetzung erlassenen nationalen Datenschutzgesetze. Mit dem 25.05.2018 wird sie auf Unternehmen und Behörden als Verantwortliche für die DV (künftig: Verantwortliche) unmittelbar anwendbar.

Die VO wird neben der Privatwirtschaft grundsätzlich auch den hoheitlichen Bereich betreffen. Es gibt jedoch Ausnahmen, z.B. für die Tätigkeiten der Gerichte, der Staatsanwaltschaften sowie der Polizei. Umgekehrt gilt die VO generell für alle bundes-, landes- und kommunalrechtlichen Aufgabenbereiche - jedoch mit zahlreichen „Öffnungsklauseln", die es den Mitgliedstaaten erlauben, im öffentlichen Bereich eigene, spezifischere Bestimmungen zur Konkretisierung der VO einzuführen.

Um die uneingeschränkte Anwendbarkeit der VO zu gewährleisten, müssen die Mitgliedstaaten teilweise ihr nationales Recht anpassen. In Deutschland kommt diese Aufgabe in erster Linie dem Gesetzgeber zu. Aber auch die Selbstverwaltungskörperschaften - insbes. die Kommunen und die Hochschulen - sind aufgefordert, ihr Satzungsrecht mit der VO in Einklang zu bringen.

Bis zum 25.05.2018 müssen somit alle Dokumente und Prozesse der Datenverarbeitung (DV) an angepasst sein.

Die VO ergänzt die NIS-Richtlinie der EU und deren Vorbild, das deutsche IT-Sicherheitsgesetz von 2015, die - zusammen mit weiterer europäischer IT-Sicherheitsgesetzgebung - die künftige Basis für ein einheitliches Datenschutz-/ Datensicherheitsrecht für Europa bilden. Hauptziele sind hierbei die Sicherstellung der öffentlichen Infrastrukturen, der Schutz bedeutender Wirtschaftsgüter und die Bekämpfung von Cyberkriminalität. Im Verhältnis zum Bruttoinlandsprodukt sind die Schäden im Bereich Wirtschaftsspionage und Cyberkriminalität nirgends so hoch wie in Deutschland.

1. „Unentrinnbar“(1) – der weite geographische Anwendungsbereich der EU-DSGVO

Die VO wird sich auf alle Unternehmen auswirken, die geschäftlich von der EU aus tätig sind bzw. Geschäftsbeziehungen zu Unternehmen und Organisationen mit Sitz in der EU unterhalten oder ihre Daten in EU-Mitgliedsstaaten sammeln, verarbeiten und speichern (lassen). Damit erstreckt sich die VO auch auf Verarbeiter mit Sitz außerhalb der EU.

Sie findet geografisch insbes. Anwendung für jede DV innerhalb der EU sowie des Weiteren für Verarbeitungen von personenbezogenen Daten (pD) durch die EU-Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters, unabhängig vom „Wo“ - also davon, ob die DV selbst auch innerhalb des EU-Gebietes stattfindet. Des Weiteren kommt sie zur Anwendung bei der Verarbeitung der pD von EU-Bürgern durch Auftraggeber („Data Controller“) oder Auftragnehmer („Data Processor“) auch außerhalb der EU, sowie ferner bei der DV durch Auftraggeber außerhalb der EU, sofern es sich um Angebote von Onlineshops, die auch auf Vertragsabschlüsse in der EU gerichtet sind, handelt, gleichgültig ob diese Angebote kostenpflichtig oder kostenfrei sind. Sie gilt des Weiteren bei Waren- oder Dienstleistungsangeboten an EU-Bürger (wobei dieses Falls ein Vertreter in der EU benannt werden muss), ferner bei Profiling außerhalb der EU, sofern Zielobjekte Bürger in der EU sind, und schließlich - gleichsam als Auffangnorm - immer dann, wenn für die betreffende DV das Recht eines EU-Mitgliedsstaates greift - im Grunde also nahezu immer.

Die VO wird demnach erhebliche Konsequenzen auch für nicht-europäische Unternehmen haben, die in der EU tätig sind, da Hauptanknüpfungspunkt die Geschäftstätigkeit bzw. das Handeltreiben in den Mitgliedstaaten der EU ist.

Da die VO kein dispositives Recht darstellt, das von Vertragsparteien für ihren Datenaustausch vertraglich ausgeschlossen werden könnte, ist aus dem Anwendungsbereich der VO sprichwörtlich „kein Entrinnen“, was auch für UK im Zeitalter nach dem Vollzug des BREXIT gelten wird.

2. „Unentrinnbar“(2) – die extensive Auslegung des Anwendungsbereichs „personenbezogene Daten“ im Sinne der EU-DSGVO

Betroffen von der VO sind alle Organisationen, die pD sammeln, verarbeiten und speichern. Laut Definition handelt es sich bei pD um sämtliche Informationen über eine Person, gleichgültig ob sich diese auf deren Privat- oder Berufsleben beziehen. Dazu zählen bspw. Namen, Fotos, E-Mail-Adressen, Bankdaten, Beiträge auf Social-Networking-Websites, medizinische Daten - sowie auch die IP-Adressen, selbst wenn diese dynamisch sind. Denn es ist ausreichend, wenn die Verantwortlichen über „rechtliche Mittel“ verfügen, die ihnen die Bestimmung der hinter der IP-Adresse stehenden Person grundsätzlich ermöglichen. Irrelevant wird damit, ob die Zuordnung zu einer bestimmbaren Person im konkreten Fall wirklich erfolgt, sondern lediglich, ob die rechtlichen Mittel die Verantwortlichen allgemein hierzu in die Lage versetzen. Lediglich im Falle absolut nicht rückführbarer, anonymer (z.B. rein statistischer oder durch Verschlüsselung nach dem Stand der Technik entpersonalisierter) Daten scheidet eine Anwendbarkeit der VO aus. Die insbes. für zulässige Durchführung und Vertrieb von Industrie 4.0 (I4.0) und Big Data-Projekten und -Produkten benötigte Lösung liegt also in Verfahren, die eine absolute Anonymisierung zuverlässig sicherstellen, so dass niemand - auch kein externer „Superuser“ - mehr in der Lage ist, die entsprechend bearbeiteten Informationen einer konkreten Person zuzuordnen. Nur wenn ein Personenbezug sonach „absolut nicht herstellbar“ ist, handelt es sich um im Rechtssinne anonyme Daten, auf die das Datenschutzrecht keine Anwendung findet.

3. Die wichtigsten Neuerungen

An wesentlichen Neuerungen gegenüber dem herkömmlichen europäischen Datenschutzrecht sind - neben den noch im Einzelnen zu erläuternden Maximen des „Datenschutzes durch Technik" („Privacy by Design") bzw. der „datenschutzfreundlichen Voreinstellungen" („Privacy by Default") und des Rechts- und Kontrollinstituts der „Datenschutz-Folgeabschätzung" (DFA) - insbes. zu nennen die Rechte auf Vergessenwerden, auf Datenberichtigung, auf Löschung, Sperrung und Datenportabilität sowie die Verpflichtung zur Notifizierung von Datenschutzverletzungen. Die Dokumentationspflichten werden inhaltlich deutlich erweitert und zudem künftig auf den Auftragsverarbeiter erstreckt. Durch die VO kommt es zudem wie gesehen zu einer Erweiterung der Anwendbarkeit von EU-Datenschutzvorschriften auf die Auftragsverarbeiter und deren Auftraggeber in Drittstaaten. Neu ist auch, dass Auftragsverarbeiter künftig für Datenschutzverletzungen bei ihrer Auftrags-DV (ADV) in die (Mit-) Haftung genommen werden können; im Einzelnen:

4. Auftragsverarbeitung: Neue Haftungskonzepte bei Cloud & Co.

Eine ADV ist nur zulässig, wenn ein Gesetz dies gestattet oder ein schriftlicher bzw. elektronischer Vertrag diese detailliert regelt. Der Auftragsverarbeiter ist sorgfältig nach Kriterien wie Zuverlässigkeit, Leistungsfähigkeit und seinen dem Stand der Technik entsprechend zum Einsatz kommenden technisch-organisatorischen Sicherheitsmaßnahmen auszuwählen und sodann vor sowie regelmäßig während der Laufzeit der ADV zu kontrollieren.

Der entsprechende Vertrag muss bestimmte inhaltliche Mindestanforderungen erfüllen. Wie bisher darf der Auftragsverarbeiter die Daten nur auf Weisung des Verantwortlichen verarbeiten. Allgemein gilt, dass in Fällen, in denen sich ein Auftragsverarbeiter nicht an die Beschränkungen der ihm vorgegebenen Verwendung der Daten hält, er insoweit selbst zum - dann rechtswidrig agierenden - Verantwortlichen „mutiert". Der ursprüngliche Auftraggeber kommt seinerseits in Erklärungsnot, warum und wie der Auftragsverarbeiter gegen seinen Auftrag verstoßen konnte. In derartigen Fällen ist von einer gemeinsamen (auch haftungs-) rechtlichen Verantwortung auszugehen. Eine wichtige Konsequenz der gemeinsamen Verantwortung liegt dann in der gesamtschuldnerischen Haftung für alle Schadensfolgen:

Bei Verstößen gegen die Bestimmungen der VO zur ADV trifft die Haftung daher im Zweifel alle an der DV (Mit-) Verantwortlichen. Zivilrechtlich haften der Verantwortliche und der Auftragsverarbeiter gegenüber den Betroffenen grundsätzlich gemeinsam und gesamtschuldnerisch. Jedoch beschränkt sich die Haftung des Auftragsverarbeiters auf speziell ihm auferlegte Pflichten (es sei denn er habe sich über die Weisungen des Verantwortlichen hinweggesetzt). Auch die Bußgelddrohungen richten sich sowohl gegen den Verantwortlichen wie auch den Auftragsverarbeiter.

In diesem Zusammenhang sei daran erinnert: Bei RZ-Betrieb, ASP, SaaS, Hosting und Cloud handelt es sich ausnahmslos um eine solche ADV-Konstellation im Sinne der VO.

Nach neuem Recht kann eine ADV auch außerhalb der EU stattfinden, wobei die VO hierbei wie gesehen gleichwohl anwendbar ist und bleibt. Die VO eröffnet den Verantwortlichen für ihren Datenaustausch (d.h. alle Übermittlungen von pD, insbes. im Falle der ADV) mit „unsicheren Drittstaaten", in denen kein angemessenes Datenschutzniveau festgestellt werden kann, bestimmte Legitimationsgrundlagen. Als solche kommen namentlich in Betracht die Übernahme von verbindlichen und durchsetzbaren Garantien zwischen staatlichen Stellen, unternehmensweite verbindlichen Datenschutzregelungen („Binding Corporate Rules", BCR) und (wie bisher) Standarddatenschutzklauseln, sofern diese zuvor durch die EU-Kommission genehmigt wurden. Neu ist hierbei die Möglichkeit, im Rahmen von BCR nicht nur für die Mitglieder der bestimmten Unternehmensgruppe sondern auch für eine Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit - auch im Subunternehmerverhältnis und innerhalb einer Kunden-/ Lieferantenbeziehung - verfolgen, untereinander und wechselseitig eine Legitimationsgrundlage für den Datenaustausch schaffen.

5. Datenschutz-Folgeabschätzung

Die VO verlangt ferner zeitgemäße, effektive Datenschutz- und Datensicherheitskonzepte sowie - als neues, dem Datenschutzrecht bislang fremdes Rechtsinstitut - die schon erwähnte DFA, wenn mit Anwendung oder Einführung von neuen IT-Verfahren ein hohes Risiko für Rechte und Freiheiten der Betroffenen verbunden ist. Bei allen Alt- und auch kommenden Neuprojekten aus dem Bereich der IT muss zumindest angeprüft (und dies entsprechend dokumentiert) werden, ob eine DFA notwendig ist.

Das Management muss mithin Strukturen schaffen, die sicherstellen, dass DFAs umfassend und ordnungsgemäß durchgeführt und dokumentiert werden. Eine Dokumentation ist in jedem Falle anzufertigen, also auch dann, wenn die Abwägung dazu geführt hat, dass eine DFA nicht durchzuführen ist.

Die mit diesen Bewertungen zwangsläufig verbundene Rechtsunsicherheit wird dadurch abgemildert, dass die VO die Datenschutzaufsichtsbehörden verpflichtet, entsprechende Listen zu veröffentlichen, in welchen Fällen eine DFA im Zweifel erforderlich ist.

6. Datenschutzkonzept und technisch-organisatorische Datensicherheitsmaßnahmen

Die Regelungen der VO über die Datensicherheit sind zum Gutteil den inländischen Regelungen des BDSG nachempfunden. Verlangt wird u.a. ein angemessenes Datenschutzkonzept. Der Verantwortliche muss durch technisch-organisatorische Strategien und deren Umsetzung sicherstellen und nachweisen können, dass er die VO einhält. Es besteht die Möglichkeit eines solchen Nachweises durch Zertifizierung oder die behördliche Genehmigung von BCR.

Die technischen und organisatorischen Maßnahmen für die Datensicherheit sollen grundsätzlich auf Basis einer Risikobewertung erfolgen. Ähnlich wie im bereits aus dem Aktien- und Handelsrecht bekannten Teilbereich der „Corporate Governance" mit den dortigen Rechtspflichten für ein effizientes Risikomanagement (und ein hierauf bezogenes internes Kontrollsystem) soll diese Risikobewertung dokumentiert sein. Gleiches gilt für die hieraus abgeleiteten Maßnahmen in Bezug auf die IT-Sicherheit und insbes. für von der IT ausgehende unternehmensgefährdende Risiken durch Datenverlust oder Verletzungen des Datengeheimnisses und des geschäftlichen Geheimnisschutzes.

Die Maßnahmen sollen dabei den aktuellen Stand der Technik für bestimmte Sektoren und Datenverarbeitungssituationen sowie die technologische Entwicklung berücksichtigen. Eine frühzeitige und regelmäßige Soll-/ Ist-Analyse mit Risikobewertung und mit einer entsprechenden Datenschutz-/ Datensicherheits-Folgeabschätzung ist aus diesem Grunde dringend anzuraten. Diese Gap-Analyse ist ein wichtiger Baustein bei der Umsetzung der in der VO postulierten Transparenz-, Dokumentations-, ADV- und Sicherheitsmanagementpflichten. In einem ersten Schritt der Gap-Analyse sollten alle von der Umsetzung der VO betroffenen Organisationseinheiten und Prozesse und rechtlichen Einheiten identifiziert werden.

7. Datenschutz durch Technik

Die VO orientiert sich an den Maximen des „Datenschutzes durch Technik" („Privacy by Design") und der „datenschutzfreundlichen Voreinstellungen" („Privacy by Default", z.B. bei Formularen und Erklärungen, etwa im Rahmen von Einwilligungen). Der Grundsatz des Datenschutzes durch Technik verlangt, dass der Datenschutz während des gesamten Lebenszyklus der Technologie „eingebaut" sein muss, von der frühesten Entwicklungsphase über ihre Einführung und Verwendung bis zur endgültigen Außerbetriebnahme. Die Ermittlung der Risiken und die hieraus abzuleitenden Maßnahmen zu deren Eindämmung sind also bereits im Vorfeld des Einsatzes der Technik konzeptionell zu entwickeln und dokumentieren. Sie müssen ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

8. Benachrichtigungspflichten bei Verstößen

Künftig muss jede Datenschutzverletzung grundsätzlich unverzüglich, spätestens jedoch binnen 72 h nach Kenntniserhalt den Aufsichtsbehörden gemeldet werden. Ausgenommen sind solche Fälle, in denen den der Verantwortliche nachweist, dass kein Risiko für Rechte und Freiheiten der Betroffenen besteht. Will er Bußgelder ausschließen, muss er einen belastbaren Prozess für das Meldemanagement aufsetzen - oder grundsätzlich jede Datenschutzverletzung melden. Unternehmen müssen Verletzungen und entsprechende Risikoprognosen ohnehin ausnahmslos dokumentieren (vgl. RMS, IKS nach AktG und HGB, SoX, SEC etc.).

Ähnlich dem deutschen Vorbild in § 109a TKG sind Verlautbarungspflichte („Data Breach-Notifications") vorgesehen, insbes. bei Sicherheitsvorfällen. Eine Benachrichtigung der Betroffenen entfällt, wenn der Aufsichtsbehörde nachgewiesen wird, dass geeignete technische Sicherheitsvorkehrungen getroffen wurden. Bei ausreichenden Sicherheitsmaßnahmen und/ oder regelmäßiger Verschlüsselung der Daten oder Beseitigung der Gefahr ist eine Meldung an die Aufsichtsbehörde nicht erforderlich. Die VO gewährt also eine Privilegierung durch IT-Sicherheit.

9. Betriebliche und behördliche Datenschutzbeauftragte

Die Bestellung eines betrieblichen Datenschutzbeauftragten (bDSB) geschieht künftig auf freiwilliger Basis, es sei denn die Bestellung sei durch EU- oder nationales Recht gefordert. Dies ist freilich in den meisten EU-Mitgliedsstaaten der Fall, jedoch mit unterschiedlichen Eintrittsschwellen nach Unternehmensgröße. Deutschland wird die bisherige Verpflichtung zur Bestellung eines bDSB beibehalten. Öffentliche Stellen haben, sofern sie pD verarbeiten, nun stets einen DSB zu bestellen.

Ebenfalls neu ist die Auferlegung einer Kontroll-/ Überwachungsfunktion gegenüber dem Management anstelle der bisherigen (bloßen) Hinweispflicht. Die Rolle des bDSB wird mithin durch die VO künftig gestärkt (wenngleich er auch weiterhin ohne Weisungskompetenz bleibt); spiegelbildlich trifft allerdings - neben Management, CIO und Compliance-Officer - nun auch ihn ein Haftungsrisiko, sofern er seinen gesetzlichen und sonstigen Pflichten nicht ordnungsgemäß nachkommt.

10. Geldbußen, Schadensersatz, Verarbeitungsstopp: Verschärfte Sanktionsmittel

Mit Inkrafttreten der VO drohen Unternehmen, ihrem Management (und ggfls. auch den Kontrollgremien wie insbes. dem Aufsichtsrat) und ihren Sonderbeauftragten für Compliance, Datenschutz und Informationssicherheit nochmals deutlich höhere Gefahren einer haftungsrechtlichen Inanspruchnahme als bislang.

Die VO stellt allgemein die Forderung auf, dass Sanktionen wirksam, verhältnismäßig und abschreckend sein müssen. Sie gibt den Bußgeldrahmen vor und erweitert gegenüber dem bisherigen Recht den Freiheitsstrafrahmen. Sanktionen sind im Ergebnis zumeist mit Haftung gleichzusetzen. Haftung impliziert im Falle der VO die volle Bandbreite zivilrechtlicher und öffentlich-rechtlicher Sanktionen. Umfasst sind insbes. Kriminalstrafen (Geldstrafe, Freiheitsstrafe), Verwaltungsstrafen/ Bußgelder und Ordnungsmaßnahmen, die über die Unterlassung bestimmter (Geschäfts-) Handlungen und DV-Vorgänge bis zur Stilllegung des Betriebs führen können.

Die Haftung kann sich auch auf natürliche Personen erstrecken. Beschränkt sich die Bußgeldforderung auf das Unternehmen selbst, wird das zuständige Kontroll- und Aufsichtsgremium freilich dennoch gehalten sein, Regressansprüche gegen die verantwortlichen Personen geltend zu machen.

Zivilrechtliche Ansprüche sind demgegenüber in der Regel gerichtet auf Schadensersatz. Ansprüche, die aus der Verletzung der VO entstanden sind, beinhalten auch die reinen Vermögensschäden (wie insbes. den entgangenen Gewinn); hierbei gibt es keinerlei Haftungshöchstgrenze. Der Berechnungsansatz für die Bußgelder, die aufgrund von Verstößen gegen die

VO verhängt werden können, ist der weltweite Konzernumsatz. Sie werden in zwei Stufen bemessen (wobei für den Fall ihrer Uneinlänglichkeit ersatzweise die Möglichkeit einer Freiheitsstrafe eröffnet ist), und zwar auf Stufe 1 für allgemeine Verstöße (z.B. gegen die VO-Bestimmungen zur ADV) bis 10 Mio. Euro oder 2 % des weltweiten Umsatzes, davon der höhere Betrag, auf Stufe 2 (Verletzung der Grundsätze der DV, z.B. bei unwirksamer Einwilligung; Verletzung von Betroffenenrechten; Verstöße gegen Bestimmungen des internationalen Datentransfers; Regelungen von Mitgliedsstaaten wie etwa im Bereich des Mitarbeiterdatenschutzes; Nichtbefolgung von Anweisungen oder Auflagen) bis 20 Mio. Euro oder 4 % des weltweiten Umsatzes, davon der höhere Betrag, und Bisher reichten in Deutschland die Bußgelder nur bis 300 TEUR bei materiellen Datenschutzverstößen und 50 TEUR bei formellen Verstößen. Neu ist der Strafrahmen bis zu 3 Jahren für Fälle, in denen der Verantwortliche wissentlich nicht allgemein zugängliche pD einer großen Zahl von Personen, ohne hierzu berechtigt zu sein, einem Dritten übermittelt oder auf andere Art und Weise zugänglich macht und hierbei gewerbsmäßig handelt.

11. Auswirkungen auf Industrie 4.0 und Big Data

Die Schlagworte Internet of Things (IoT) und Industrie 4.0 (I4.0) stehen - vereinfacht dargestellt - für neue, innovative Geschäftsmodelle, die möglich werden durch rasante technische Entwicklungen in den Bereichen Vernetzung von Endgeräten, autonome „Maschinenentscheidungen" durch Systeme der künstlichen Intelligenz (KI) und Auswertbarkeit großer Datenmengen durch hochleistungsfähige Computersysteme (Big Data/HPC). Die Auswertung und Steuerung solcher Systeme erfolgt durch Datenaustausche, die sich zumeist über Ländergrenzen hinweg vollziehen.

Big Data, I4.0 und KI-Verfahren müssen daher von vornherein international-datenschutzrechtlich bis ins Detail durchgeplant werden, dies insbes. unter Einschluss der neuen datenschutzrechtlichen Verpflichtungen zu „Privacy by Design/ Default" und der DFA. (Etwas anderes gilt wie gesehen bei Aufhebung der Personenbeziehbarkeit. Da dies die absolute Anonymisierung „gegenüber jedermann" erfordert, bedarf es hierfür einer effektiven und zeitgemäßen Verschlüsselung und deren Dokumentation).

Denn bei den datenschutzrelevanten Handlungen, auf die die VO Anwendung findet, handelt es sich um die Erhebung, Verarbeitung und Nutzung von pD, wobei Unterkategorien der Verarbeitung die Speicherung, Übermittlung, Veränderung, Sperrung und Löschung sind und es sich bei dem Nutzungsbegriff um den Auffangtatbestand jeder sonstigen Verwendung handelt. Damit unterliegt die gesamte DV-Wertschöpfungskette den Datenschutzgesetzen, von der Generierung/ Erhebung bis zur Löschung.

Für das Design von KI, Big Data und I4.0-Prozessen ist ferner auf weitere bestimmende Prinzipien des EU-Datenschutzrechts Rücksicht zu nehmen, namentlich das grundsätzliche Verbot der DV von pD Daten mit Erlaubnisvorbehalt, den Zweckbindungsgrundsatz und die Notwendigkeit einer Rechtfertigung (Gesetz, Einwilligung), die wiederum in Wechselwirkung mit dem bestimmten Verwendungszweck steht. Dies bedeutet, dass eine Verwendung einmal vorhandener Daten zu anderen Zwecken oder die Zusammenführung von Daten mit Daten aus anderen Quellen oder jede Zweckänderung einer neuen, zusätzlichen Rechtfertigung bedarf.

Dies führt bei diesen Prozessen häufig zu Problemen, da Daten aus ihrem ursprünglichen Zweckzusammenhang gerissen, zusammengeführt, umstrukturiert und analysiert und damit neuen Nutzungen zugeführt werden müssen. Eine individuelle Einwilligung erscheint hier mit Blick auf die hohen Wirksamkeitshürden nicht praktikabel. Die Einwilligung wäre nur dann wirksam, wenn sie auf einer hinreichend informierten Grundlage erklärt wurde und den Bestimmungen des AGB-Rechts, insbes. dem Transparenzgebot, genügen würde. Als weiteres Manko kommt die jederzeitige Widerruflichkeit der Einwilligung hinzu.

Soweit also gesetzliche Rechtfertigungstatbestände zur Verfügung stehen, sollten diese für I4.0-Verfahren primär genutzt werden. Alternativ bedürfte es eines Vertragsmanagements, das gewährleistet, dass die jeweilige DV für die Anbahnung und Erfüllung eines Vertrages mit dem oder den Betroffenen erforderlich ist, sodass eine entsprechende Gestaltung der Vertragsbeziehungen zweites Mittel der Wahl ist. Erst wenn und soweit gesetzliche Rechtfertigungsbestände nicht eingreifen, sollte auf das Instrument der Einwilligung zurückgegriffen werden.

12. IT-Sicherheitsgesetzgebung in Deutschland und Europa

Wie Statistiken belegen, müssen 70% der Unternehmen, bei denen es zu Datendesastern kommt, innerhalb von 18 Monaten ihren Betrieb einstellen. Im Bereich Wirtschaftsspionage belaufen sich allein in Deutschland, dem wichtigsten Angriffs- und Spionageziel in der EU, die Schäden auf jährlich 51 Mrd. Euro, weltweit werden diese laut Europol auf 290 Mrd. Euro geschätzt. Cyberangriffe erfolgen dabei meist noch nicht einmal überwiegend, um an bestimmte Informationen zu gelangen - die Mehrzahl der Fälle zielt auf reine Sabotage.

Konjunktur haben bei der neuen Cyberkriminalität insbes. Methoden, die Schadcode über das Internet durch Webseiten und Dienste unbeteiligter Dritter verbreiten. Nach Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) gehören diese Verbreitungsformen zu den größten Bedrohungen der Netzsicherheit: 75 % der Webseiten werden als verwundbar eingestuft. Beim ungewollten Hosten von Malware auf Webseiten liegt Deutschland weltweit an zweiter Stelle.

Schätzungen zufolge belaufen sich die Schäden, die allgemein durch Cybercrime eintreten, weltweit auf 400 Mrd. Dollar. Gemessen am Bruttoinlandsprodukt ist Deutschland seit Jahren trauriger Spitzenreiter für Angriffe und Schäden im Bereich der IT.

Die überwältigende Vielzahl von Sicherheitsvorfällen dringt aus Gründen der Unternehmensraison nicht an die Öffentlichkeit. Daher sind keine verlässlichen Zahlen zu einzelnen Schäden durch interne IT-Pannen (fehlerbedingte HW/ SW-Ausfälle, Mitarbeiter-/ Wartungsfirmenversagen etc. ohne Dritt-/ Außeneinwirkung durch z.B. Hacking, DoS, Malware etc.) zu erhalten. Jedoch gibt es Ausnahmen, die der Prominenz der betroffenen Unternehmen, aber auch der weiten Betroffenheit der Nutzergemeinde und den damit einhergehenden Verlautbarungspflichten geschuldet sind:

12.1. Prominente Desasterfälle

An aufsehenerregenden Rechtsfällen ist bspw. das Daten-Desaster im Cloudservice „Amazon EC 2" aus dem April 2011 zu nennen, bei dem eine unbekannte Datenmenge unwiederbringlich verloren ging. Ähnliches war bei einem anderen Cloudservice schon im Oktober 2009 geschehen: Ein Serverfehler hatte zu umfangreichen Datenverlusten bei Nutzern des Dienstes „Sidekick", den T-Mobile gemeinsam mit der Microsoft-Tochter Danger anbot, geführt. Abermals die Telekom-Gruppe stand im Herbst 2010 in der Kritik für Datenverluste in ihrem Email-Center. Dem Vernehmen nach waren Einstellungen in den Posteingangsordnern, die mit „Nie löschen" hinterlegt waren, in Folge eines Updates mit einer Standard-Vorhaltedauer von 90 Tagen überschrieben worden. Businessmails, die älter als 90 Tage waren, gingen Nutzerangaben zufolge unwiederbringlich verloren. Und auf verwaltungsrechtlicher Ebene begannen im März 2016 Landesdatenschutzbehörden damit, Bußgeldverfahren gegen Unternehmen einzuleiten, die - nach dem Wegfall von „Safe Harbor" als Rechtsgrundlage für den Datenaustausch mit den USA durch ein Urteil des EuGH vom 06.10.2015 - weiterhin pD zur DV in die USA transferierten.

12.2. IT-Sicherheitsgesetz: KRITIS-Betreiber und Internetdienste

Vor dem Hintergrund der allgemeinen Bedrohungslage wurden durch das seit dem 25.07.2015 in Kraft stehende IT-Sicherheitsgesetz (IT-SiG) bestimmten Branchen (sog. „Sektoren", nämlich Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen) und Kategorien von Unternehmen (Betreiber kritischer Infrastrukturen/ KRITIS, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil ihr Ausfall oder ihre Beeinträchtigung zu erheblichen Versorgungsengpässen oder Gefährdungen der öffentlichen Sicherheit führen würde) mannigfaltige Verpflichtungen in Bezug auf die Sicherheit ihrer Systeme und Daten auferlegt.

Darüber hinausgehend wurden allgemein alle geschäftsmäßigen Anbieter von Telemediendiensten zur Umsetzung von Sicherheitsmaßnahmen nach dem Stand der Technik verpflichtet. Dies betrifft nahezu sämtliche nicht dem rein privaten Bereich zuzurechnenden Internet-Angebote wie Webshops, Online-Auktionshäuser, Suchmaschinen, Webmailer, Informationsdienste, Podcasts, Chatrooms, Social Communities, Webportale und Blogs. Zentraler Gesetzeszweck ist die

Fortsetzung der nationalen und - beispielsweise auf EU-Ebene - internationalen Bestrebungen, Betriebsausfälle und Haftungsrisiken gesetzgeberisch bestmöglich zu begrenzen.

12.3. IT-Sicherheitsmanagement, Meldepflichten und Sanktionen

KRITIS-Betreibern wird auferlegt, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen KRITIS vor dem Hintergrund der Schutzziele Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von IT-Systemen und Prozessen maßgeblich sind. Anforderungsmaßstab ist der jeweilige „Stand der Technik". Die Unternehmen stehen in der Pflicht, ihre Sicherheitstechnik fortlaufend zu überprüfen und zu aktualisieren, insbes. also für zeitnahe Sicherheits-Updates zu sorgen. Gleichzeitig müssen die Auswirkungen der Maßnahmen beherrschbar bleiben. KRITIS-Betreibern wird mithin eine Technikfolgenabschätzung auferlegt.

IT-Sicherheitsvorfälle sind dem BSI zu melden, um die Erstellung eines IT-Sicherheitslagebildes zu ermöglichen und sämtliche Betreiber frühzeitig warnen zu können. Namentlich Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse sind unverzüglich zu melden. Erfasst werden auch erfolgte, versuchte oder auch erfolgreich abgewehrte Angriffe im Rahmen von Cyberkriminalität.

Bei (auch fahrlässigen) Verstößen gegen Verpflichtungen des IT-SiG kann das BSI Bußgelder (je nach Verstoß bis 50 bzw. 100 TEUR) verhängen. Der Sanktionskatalog sieht Bußgelder bereits vor für die nicht erfolgte, nicht richtige, nicht vollständige oder nicht rechtzeitige Meldung bereits eingetretener Sicherheitsverletzungen. Haftungsrechtlich erlangt die Frage der Einhaltung der Sicherheitsanforderungen Bedeutung für Schadensersatzansprüche von Vertragspartnern und geschädigten Dritten. Auch eine - besonders schadensträchtige - Haftung gegenüber anderen KRITIS-Betreibern kommt in Betracht, so etwa wenn diese infolge einer Verletzung von Meldefristen nicht mehr rechtzeitig vom BSI gewarnt werden konnten, wenn Angreifer Systeme hacken und auf Komponenten zugreifen können, von deren Funktionsfähigkeit mehrere Betreiber abhängig sind, oder wenn mangelhafte IT-Sicherheit es Unbefugten ermöglicht, Daten auszulesen und mit diesen Daten die Systeme anderer Betreiber missbräuchlich zu nutzen.

Für geschäftsmäßige Internetdienste wurde die Rechtslage ebenfalls unter IT-sicherheitsspezifischen Aspekten verschärft mit dem Ziel, die Verbreitung von Schadsoftware über Webseiten - die wie eingangs gesehen zu den wirtschaftlich bedeutsamsten Bedrohungen der Netzsicherheit zählt - einzudämmen, indem den Anbietern technische und organisatorische Vorkehrungen zum Schutz des Zugriffs auf ihre Angebote - wiederum nach dem „Stand der Technik" - auferlegt werden. Exemplarisch wird der Einsatz von Verschlüsselungstechniken genannt. Weitere Maßnahmen können beispielsweise das Scannen gehosteter Daten oder die Installation von Firewalls sein. In organisatorischer Hinsicht sind geeignete Berechtigungskonzepte für Zugangs- und Administrationsrechte zu fordern, ferner Schulungen und die Einräumung vertraglicher Kontrollmechanismen. Auch ein Outsourcing der Sicherheitsmaßnahmen an spezialisierte Dienstleister sowie deren Überwachung und Kontrolle beispielsweise durch Audits oder die Vorlage von Zertifikaten unabhängiger Prüforganisationen sind in diesem Kontext zu nennen.

Verstöße sind mit bis zu 50 TEUR bußgeldbewehrt. Weitere hoheitliche Sanktionen reichen bis zur Untersagung und Sperrung der Dienste. Haftungsrechtlich bestehen gegenüber den Nutzern Schadensersatzpflichten aus Vertragsverletzung und - außerhalb einer vertraglichen Beziehung - aus unerlaubter Handlung aufgrund sog. „Verkehrssicherungspflichtverletzung".

12.4. NIS-Richtlinie der EU

Weitere spezifische IT-Sicherheitsregelungen, die entsprechende Schutzvorkehrungen vorschreiben, sind in diversen Gesetzeswerken verteilt und betreffen in der Regel einzelne, besonders schützenswerte Teilbereiche der Wirtschaft bzw. bestimmte Kategorien von Daten. Staatenübergreifend ist hier exemplarisch die EU-Richtlinie zur Informations- und Netzsicherheit aus dem Februar 2013 (NIS-Richtlinie) zu nennen: Neben dem Energie-, Banken-, Verkehrs- und Gesundheitsbereich („Betreiber wesentlicher Dienste") werden auch Internetdienste wie Suchmaschinen, Cloudanbieter und

Plattformbetreiber verpflichtet, Maßnahmen zu ergreifen, um ihre Widerstandsfähigkeit gegen Cyberangriffe zu verbessern, größere Zwischenfälle den nationalen Behörden zu melden - und diese unter bestimmten Voraussetzungen auch zu veröffentlichen.

12.5. Mindestanforderungen an die IT-Sicherheit

Es lassen sich insgesamt wichtige gemeinsame technische und organisatorische Standards wie Verschlüsselung, konfigurationsfehlerfreie Internet- und spezielle Sicherheitssoftware (Firewall, Malware-Scanner, „Intrusion Detection" und „Data Loss Prevention"), Backup- und „Information Security Management"-Systeme", fortlaufend zu aktualisierende Datenschutz-/ Datensicherheitskonzepte (inkl. Maßnahmen zur Angriffsprävention und „Desaster Recovery/ Business Continuity"-Management) als Stand der Technik und Best Practice herausfiltern.

Angesichts des sprunghaften Anstiegs der Cyberkriminalität und den mit ihr verbundenen Milliardenverlusten der Wirtschaft kommt hierbei in organisatorischer Hinsicht geeigneten Notfallplänen, in denen Reaktionen auf Angriffe und Desaster-Szenarien festzulegen und in regelmäßigen Abständen Notfälle testweise zu simulieren sind, besondere Bedeutung zu.

Die getroffenen technischen und organisatorischen Vorkehrungen sind zu dokumentieren und nach dem Maßstab des Standes zu bewerten, damit gegebenenfalls ein sachkundiger Dritter die umgesetzten Maßnahmen substanziell überprüfen und ein Gericht zu einem Urteil hinsichtlich der Verantwortlichkeiten im verkehrssicherungspflichtigen oder nebenvertraglichen Bereich gelangen kann.

12.6. IT-Security-Rechtsprechung

Auch die Rechtsprechung unterstreicht, dass eine zuverlässige IT-Sicherheit in Bezug auf betriebskritische Daten zu den unternehmerischen Selbstverständlichkeiten im Zeitalter digitaler DV gehört. Aus der inländischen Judikatur, bei der zumeist Haftungstatbestände im Zusammenhang mit dem Verlust betriebswichtiger oder dem fahrlässigen Bruch der Vertraulichkeit geheimhaltungsbedürftiger Daten Anlass für - auch persönliche (Managerhaftung) - Schadensersatzansprüche waren, sind insbes. die folgenden Aussagen von besonderer Relevanz für die Unternehmenspraxis:

- Die Rechtsprechung sieht die Sicherheit der Kommunikation als Compliance-relevante Verpflichtung an. Unternehmenskritische - und insbes. auch beweiserhebliche - Dokumente müssen aus Gründen der Rechtssicherheit und Beweisführung vorgehalten werden. Wird dies nicht ermöglicht, kann ein Prozess bereits unter bloßen Beweislastgesichtspunkten wegen „Beweisfälligkeit" verloren gehen.

- Ein Outsourcing der IT-Sicherheit genügt grundsätzlich nicht, das delegierende Unternehmen und dessen Management zu Lasten beauftragter IT-Unternehmen (wie z.B. Cloud-Provider oder IT-Wartungsfirmen) zu „exkulpieren", also aus der haftungsrechtlichen Verantwortung für den Schutz und die Sicherheit seiner Daten und Systeme zu nehmen. Dies kann sogar gelten bei einem Verschulden des externen IT-Dienstleisters bei einem Datenverlust, wenn das den Auftrag erteilende Unternehmen die Konsequenzen dieses Verlusts durch unzuverlässige Desaster- und Backup-Strategien mit verursacht hat. Der Mitverschuldensanteil kann hier bis zu 100 %, also bis zur Vollhaftung des Unternehmens für den entstandenen Datenverlust und damit den hierdurch verursachten finanziellen Schaden, führen.

- Zu beachten ist in diesem Kontext auch die Beweislastumkehr, wonach in Fällen, in denen streitig ist, ob die zuständigen Mitglieder des Managements die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters angewandt haben, diese zu ihrer Exkulpation die alleinige Beweislast trifft.

- Was das Desaster-Management anbelangt, verlangt die Rechtsprechung als allgemeine Schutz- und Sorgfaltspflicht, dass regelmäßig und zuverlässig zeitgemäße, lückenlose Datensicherungsroutinen im Bereich Produktivsystem, Archivsystem und Backup eingesetzt werden. Dies dürfen auch externe Fachpersonen - wie etwa mit Wartung und Support beauftragte

IT-Firmen oder Rechenzentrumsbetreiber, die im Wege der Auftragsdatenverarbeitung mit den Daten des Unternehmens arbeiten - ohne besondere Erkundigungspflicht als Selbstverständlichkeit voraussetzen. Umgekehrt sind aber diese beauftragten Dritten wiederum im Zweifel auch ohne ausdrückliche Vereinbarung zu Datensicherungsmaßnahmen wie insbesondere Backups verpflichtet, wenn die Verarbeitung von Unternehmensdaten zu ihrem Vertragspflichtenkreis gehört.

- Weiter werden zum unternehmerischen IT-Schutzpflichtenkreis revisionssichere Archivierungsprozesse gezählt, Firewalls, Filter- und Überwachungssysteme, eine Verschlüsselung jedenfalls bei besonders sensitiven Daten sowie eben auch ein Kontinuitätsmanagement, das einen Wiederanlauf nach Wiederherstellung von System und Daten im Schadensfall gewährleistet.
- Organisatorisch sind geeignete IT-Unternehmens- und Datenschutzrichtlinien sowie eine entsprechende Einweisung und Schulung der Mitarbeiter erforderlich.
- Das Fehlen eines IT-Sicherheitskonzepts berechtigt ein Unternehmen folgerichtig dazu, den mit einem Vorstandsmitglied geschlossenen Anstellungsvertrag außerordentlich und mit sofortiger Wirkung zu kündigen bzw. bei Mängeln in der Dokumentation eines Früherkennungssystems in Bezug auf dem Unternehmen drohende Risiken einen wichtigen Grund zu sehen, der zur Anfechtbarkeit des Beschlusses über die Haftungsentlastung des gesamten Vorstands führt.

Gerade auch Unternehmen mit effektiver Geschäftstätigkeit in UK und den USA sehen sich der besonderen Bedeutung (und erheblichen Sanktionsfolgen) eines lückenlosen und beweissicheren Dokumentmanagement ausgesetzt. Dementsprechend wurden die Zivilprozessordnungen beispielsweise im UK in 2010 ergänzt um Regelungen zur elektronischen Bereitstellung. Dasselbe gilt für Ergänzungen im US-Zivilprozessrecht im Jahre 2006. Im Zuge dieser Entwicklungen wurden zugleich neue Sanktionen für Vertraulichkeits- und Datenschutzverletzungen implementiert.

Zusammengefasst etabliert die Rechtsprechung zunehmend - und vor dem Hintergrund von Regelwerken mit Ausstrahlungswirkung in andere Wirtschaftsbereiche (wie etwa dem Sarbanes-Oxley-Act oder den Baseler Eigenkapitalübereinkünften) - allgemeine Sorgfaltspflichten für eine effektive, zeitgemäße IT-Sicherheit. Es lässt sich die Tendenz ersehen, eine Vorlage von Daten, auch wenn diese bereits vor langer Zeit in großen, gegebenenfalls auch externen oder auch internationalen (Backup-) Speichern abgelegt wurden und entsprechend schwer verfügbar gemacht werden können, für ein laufendes Gerichtsverfahren in einer „beweisfesten" Form zu verlangen, wobei diese Verpflichtung besteht unabhängig von gegebenenfalls höherer Gewalt oder etwaigem Fremdverschulden. Dies bedingt ggf. den Einsatz zeitgemäßer IT-Systeme, die starke Indizien für Beweissicherheit - und damit letztlich Rechtssicherheit - liefern.

Rechtssicherheit durch technische Sicherheit:

Lösungskonzepte von SEP

SEP sesam sichert businesskritische Informationen, Applikationen, Datenbanken und Systeme, welche alle Arten an Informationen von Sales- und Kundenbeziehungen über Produktion und Verwaltung bis hin zu Finanz- und Businesstransaktionen beinhalten. Aufgrund dieser immensen Wichtigkeit wird eine umfassende Business Continuity Strategie benötigt, die auf Recovery Point Objectives (RPOs) und Recovery Time Objectives (RTOs) fokussiert, welche essentiell bei einem Disaster Recovery Szenario sind.

Die einheitliche SEP sesam Hybrid Backup und Bare Metal Recovery Lösung verhindert Datenverlust und kann die gesamte Umgebung nach einem Disaster Recovery Szenario wiederherstellen wie z.B. bei:

- höherer Gewalt
- Hardware Fehlern
- Menschliche Fehler
- Datenkorruption
- Logischen und Software Fehlern

Sogar nach einer Attacke mit einem Verschlüsselungstrojaner können die SEP Backup-Daten mittels des bewährten Supports der Offline-Medien wiederhergestellt werden.

Die plattformübergreifende Hybrid Backup- und Disaster Recovery-Lösung SEP sesam ist für die Sicherung von virtualisierten und physikalischen Umgebungen optimiert und gewährleistet/ermöglicht die Einhaltung von gesetzlichen Anforderungen in heterogenen IT-Umgebungen. Verschlüsselung gehört zu den zentralen technischen Elementen. So ist z.B. bei der technologisch führenden Si3-Deduplizierung und -Replikation eine Verschlüsselung möglich. Die sichere Datenaufbewahrung wird durch die Verschlüsselung des SEP Si3-DedupStores eingeführt. Nach Zerlegen des Datenstroms in Blöcke und der Komprimierung jedes Blocks, lässt sich nun jeder einzelne Block durch einen beliebig definierbaren Key verschlüsseln. Zur Wiederherstellung der Daten kann der Key in der Datenbank des Backupservers hinterlegt werden oder der Dateneigentümer muss eine Rücksicherung mit seinem persönlichen Key autorisieren. Diese Verschlüsselung garantiert BSI-Konformität.

Desweiteren kommen eine Vielzahl technologischer Ansätze hinzu, die zur Einhaltung der rechtlichen Anforderungen beitragen.

Schlüsselelemente von SEP sesam für die gesetzeskonforme Datensicherheit:

- Verschlüsselung der Backups auf Sicherungsmedien (Band, DataStore, Si3 DedupStore)
- Verschlüsselung des Datenstromes
- Verschlüsselung der Kommunikation
- Externes Passwort für Rücksicherung nach 4-Augen-Prinzip
- Effizientes Disaster Recovery für Windows und Linux

- Frei von Spyware
- Medienbruch: Unterstützung von Offline- und WORM Medien
- Herstellerkonforme Datensicherung und –wiederherstellung
- Sicherung der Daten auf verschiedenen Ebenen möglich (z.B. auf Hypervisor- und Applikationsebene)
- Standortübergreifende Datensicherung
- Automatische Migration bzw. Kopie von Sicherungsdaten auf unterschiedliche Sicherungsmedien
- Volle Unterstützung von Open-Source Betriebssystemen auf Backupclient- und Backupserver-Seite
- Gesetzeskonforme Sicherung aller Unternehmensdaten
- Gewährt die Netzwerksicherheit in Firewall-Umgebungen durch Einschränken der Kommunikation und des Datentransports auf wenige, dedizierte Ports
- Geplanter und automatischer Restore auf Stand-by-Systeme zum Verifizieren der Backups (kann auch für Audits verwendet bzw. dokumentiert werden)
- Disaster Recovery Tests im laufenden Betrieb inklusive Reporting bei physikalischen Umgebungen (Voraussetzung ist ein Test-Target Server) und in virtuellen Umgebungen

Mit SEP sesam sind die Daten 24 Stunden/7 Tage geschützt und immer verfügbar. SEP's zuverlässige Backup-Lösung zeichnet sich durch eine Vielzahl an Zertifizierungen für namhafte Applikations-, System- und Hardwareanbieter aus (z.B. SAP, Oracle, Novell, Red Hat, Suse, Citrix, Microsoft, VMware, IBM, Fujitsu, Intel,...), d.h. durch diese Zertifizierungen wird gewährleistet, dass der original Hersteller-Support (Bsp. SAP) nicht verloren geht. Die vielseitige und ökonomische Datensicherung von SEP ist bestens geeignet für mittlere bis hin zu sehr großen Unternehmen/Organisationen und integriert sich nahtlos in jede IT Umgebung. Hierbei ist noch einmal darauf hinzuweisen, dass die technologische Lösung nur eine Komponente der gesamten "Compliance-Lösung" darstellen kann. Die Technik- /Software-Lösung muss an die vorher beschriebenen organisatorischen Maßnahmen/ Prozesse, Konzepte, Risiko-Analysen, Dokumentationen, etc. gekoppelt werden, um so zu einer ganzheitlichen "rechtskonformen" Lösung zu werden.

Die globale Lösung - Made in Germany

Weltweit haben sich Organisationen und Unternehmen vom Mittelstand bis Enterprise, für die Hybrid Backup Lösung SEP sesam entschieden. Als deutscher Hersteller bietet SEP, bei dem umfangreichen Thema Datensicherung, kurze Kommunikationswege um besonders in Krisensituationen schnell und zuverlässig Hilfe zu leisten

- Zuverlässige Sicherung & lückenlose Wiederherstellung sämtlicher Unternehmensdaten
- Flexibel anpassbare Lizenzmodelle
- Deutsche Qualitäts- und Produktstandards
- Attraktives Preis-Leistungsverhältnis

Abkürzungsverzeichnis:

- ADV: Auftragsdatenverarbeitung
- BCR: Binding Corporate Rules
- bDSB: betrieblicher/behördlicher Datenschutzbeauftragter
- BSI: Bundesamt für Sicherheit in der Informationstechnik
- DFA: Datenschutz-Folgeabschätzung
- DV: Datenverarbeitung
- HPC: High-Performance Computing
- I4.0: Industrie 4.0
- IoT: Internet of Things
- IT-SiG: IT-Sicherheitsgesetz
- KI: Künstliche Intelligenz
- KRITIS: Kritische Infrastrukturen
- NIS: Netz- und Informationssicherheit
- pD: personenbezogene Daten
- VO: EU-Datenschutz-Grundverordnung

Hauptsitz (EMEA):
SEP AG
Konrad-Zuse-Straße 5
D-83607 Holzkirchen
Telefon: +49 8024 46331 0
Fax: +49 8024 46331 666
E-Mail: info@sep.de

USA Ost:
SEP Software Corp.
470 Atlantic Avenue, 4th Floor
Boston, MA 02210 U.S.A.
Telefon: (+1) 617-273-8200
Fax: (+1) 617-273-8001
E-Mail: info@sepusa.com

USA West:
SEP Software Corp.
4665 Nautilus Court
Suite 502 A Boulder, CO 80301
Telefon: (+1) 303-449-0100
Fax: (+1) 877-611-1211
E-Mail: info@sepusa.com

Alle Warenzeichen und Handelsmarken sind Eigentum der jeweiligen Inhaber.

© SEP AG. All rights reserved. SEPsesam_Compliance_20180110