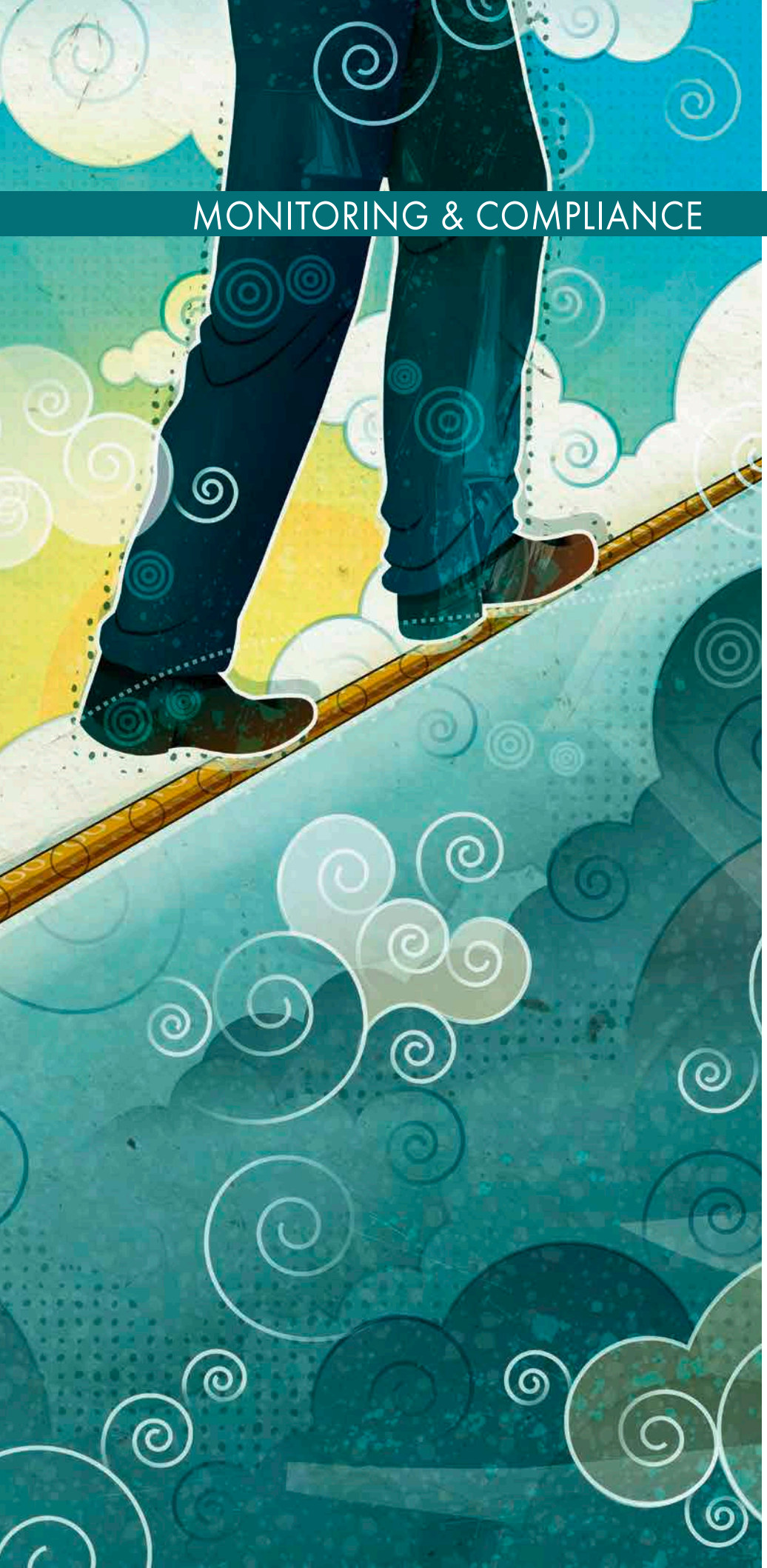

DAS DATEN-DILEMMA

So manches Unternehmen möchte nur allzugern den Verlockungen des digitalen Monitorings nachgeben, doch was technisch möglich ist, ist rechtlich nicht unbedingt erlaubt. Da gilt es Interessen abzuwägen – und neue technische Lösungen zu prüfen.

Die technischen Möglichkeiten für Monitoring- und Filterung sind in den letzten Jahren immens gewachsen (siehe Kasten), die Compliance-Herausforderungen hierbei aber auch: „Im Grunde befindet man sich in einer echten Zwickmühle“, so IT- und Datenschutz-Experte Dr. Holger Lutz aus der internationalen Anwaltssozietät Baker & McKenzie. Im Dreieck IT-Sicherheit, Datenschutz (gemäß Bundesdatenschutzgesetz BDSG und Telekommunikationsgesetz TKG) und Compliance ist die Gemengelage nicht zuletzt deswegen kompliziert, weil die Verantwortlichkeiten der jeweiligen Akteure sich überschneiden und ihre Ziele nicht unbedingt dieselben sind. Dies macht eine intensive Kommunikation und enge Abstimmung aller Beteiligten erforderlich.

Im Zuge der Vorbeugung, Entdeckung und adäquaten Reaktion auf Betrug und Unterschlagung durch Mitarbeiter („Anti-Fraud Management“) haben viele Unternehmen ihre IT- Monitoring- und Sicherungssysteme ausgebaut. Hier ist neben Spam- und Virenfilterung in erster Linie die Content-Filterung von E-Mails zu nennen, die das Verschicken von markierten

oder klassifizierten Daten an externe Adressen verhindert. Monitoringmaßnahmen sind aber auch bei Fernwartungs- und anderen Fernzugriffen auf IT-Systeme unerlässlich. Bei allen Veränderungen innerhalb des IT-Systems müsse Monitoring erfolgen, beispielsweise nach dem Vier- oder Sechs-Augen-Prinzip, empfiehlt Lukas Mempel, Konzerndatenschutzbeauftragter und Bereichsleiter Datenschutz und Datensicherheit der Sana Kliniken AG.

Aber auch bestehende Daten können nachträglich entsprechend durchsucht werden, beispielsweise im Zuge von Internal Investigations. Doch derartiges Sichten immenser Datenmengen tangiert in der Regel Persönlichkeitsrechte der betroffenen Mitarbeiter. Sind unter den E-Mails und im Instant Messaging sowie den technischen Web-Protokollen nicht nur geschäftliche Mails, sondern auch private, sind diese geschützt durch das im BDSG verankerte allgemeine Verbot zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten.

Fehlerhaftes Vorgehen kann zu Beweisverwertungsverbot führen

Nach dem TKG ist jeder Telekommunikations-Provider verpflichtet, das private Fernmeldegeheimnis zu bewahren, bei Verstoß macht er sich strafbar. Wann ist ein Unternehmen Telekommunikationsanbieter? Die vorherrschende Meinung lautet: wenn ein Unternehmen seinen Mitarbeitern die private Nutzung des Firmen-E-Mail-Accounts erlaubt oder diese zumindest duldet. Einige jüngere Gerichtsurteile weisen darauf hin, dass sich das Meinungsklima ändert, möglicherweise ein Trend zu einer liberaleren Handhabung. Gleichwohl: Wer bei seinen Monitoring-Maßnahmen nicht in Konflikt mit dem TKG kommen will, muss die private Nutzung der unternehmenseigenen E-Mai-Accounts untersagen und seine Mitarbeiter für privaten E-Mail-Verkehr auf die ausschließliche Nutzung externer, webbasierter Provider wie GMX, WEB und Google-Mail verpflichten.

Da dies in der Regel nicht geschieht, gilt: Bis zur Beendigung des Kommunikationsvorgangs muss das Unternehmen das Fernmeldegeheimnis beachten. Endet die Kommunikation, gilt das strenge deutsche Datenschutzgesetz. Entscheidende Norm ist hier der § 32 des BDSG, der den Arbeitnehmer vor ungerechtfertigter Sammlung und Nutzung seiner Daten schützt: personenbezogene Daten eines Beschäftigten zu erheben, verarbeiten oder nutzen ist nur unter engen Voraussetzungen zulässig, so beispielsweise, wenn dies der Aufdeckung einer Straftat dient und Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Für die Ermittler ist dies ein Dilemma, wie Lukas Mempel beschreibt: „Kritisch wird es immer an der Schnittstelle zwischen dem, was erforderlich ist, und dem, was ich ohne begründeten Anfangsverdacht nicht überprüfen darf." Dem Auftrag, interne Betrugsermittlungen durchzuführen, stehe entgegen, dass die

MONITORING SYSTEME

Predictive Coding™
- Stichprobe von Dokumenten wird gesichtet
- Relevante Dokumente werden erfasst und inhaltlich analysiert
- Hierauf aufbauend werden weitere Dokumente aus dem Gesamtbestand vorgeschlagen, die kontextuell zu den bereits ermittelten Treffern passen
- Suchergebnisse werden in wenigen Durchläufen verfeinert
- Sämtliche relevanten Daten werden binnen kürzester Zeit geliefert

(Quelle: Recommind GmbH)

RSA Security Analytics
- Überwacht und analysiert große Mengen sicherheitsrelevanter Daten
- Kombiniert Netzwerküberwachung, herkömmliches, protokollzentrischen Sicherheitsinformations- und Ereignismanagement (SIEM), forensische Untersuchungen, Compliance und Big-Data-Management
- Verspricht hohe Compliance: Integrierte Sicherheitsverfahren ermöglichen automatisches Handeln in Übereinstimmung mit geltenden Compliance-Vorgaben

(Quelle: EMC Deutschland GmbH)

ArcSight ESM
- Überwacht alle Ereignisse im gesamten Unternehmen
- Hochentwickelte Sammlungsfunktion für die umfangreichste Zusammenstellung von Ereignisquellen (Logs von über 275 Geräten und Ereignisquellen)
- Identifiziert auf Basis einer leistungsfähigen Korrelation und Analyse geschäftliche und technologische Bedrohungen
- Ereignisse werden in entsprechenden Kontext eingeordnet: Bei wem ist welches Ereignis wo, wann und unter welchen Umständen aufgetreten, und welche Auswirkungen hat dieses Ereignis auf das geschäftliche Risiko?
- Korrelation liefert genaue und automatisierte Priorisierung von Sicherheitsrisiken und Compliance-Verletzungen

(Quelle: ArcSight, Inc.)

Ontrack Advanceview
- Lösung zur Vorbewertung von Daten
- Visualisierte Analyse von E-Mail-Threads lässt nachvollziehen, wer mit wem zu welchem Zeitpunkt über welche Themen kommuniziert
- Erlaubt Durchsuchung des gesamten Datenvorrats zur Ermittlung entscheidender Zeiträume und Personen
- Ermöglicht auf rechtsverbindliche Weise Festlegung der Parameter für die Datenfilterung während der Verarbeitung
- Deduplizierung und Erkennung nahezu identischer Dokumente
- Schnelle Bewertung großer Mengen von Dokumenten hinsichtlich ihrer Relevanz

(Quelle: Kroll Ontrack GmbH)

Dr. Christiane Tödter, Rechtsabteilung und Drittmittelmanagement, Universitätsklinikum Heidelberg

Lukas Mempel, Konzerndatenschutzbeauftragter und Bereichsleiter Datenschutz und Datensicherheit, Sana Kliniken AG

Erhebung von Mitarbeiterdaten nur eingeschränkt zulässig ist. „Das ist nicht zuletzt auch deshalb schwierig, weil natürlich ein fehlerhaftes Vorgehen zu Beweisverwertungsverboten führen kann."
Vorzunehmen ist daher laut Strafrechtsexperte Dr. Niklas Auffermann stets eine Einzelfallabwägung, die unbedingt genau zu dokumentieren sei: „Festzulegen ist auch, wer unternehmensintern Einsicht in die Unterlagen nehmen kann, wie lange diese gespeichert werden, und wie die Auskunfts- und Informationsrechte des Betroffenen geregelt werden." Dies werde laut Aufferman oft vergessen.

Abstimmung zwischen internen Ermittlern und Datenschutzbeauftragten sollte eng sein

Da das BDSG in der Regel unbestimmte Rechtsbegriffe verwendet, ist der Verhältnismäßigkeitsgrundsatz im Einzelfall wichtigstes Kriterium für eine angemessene Entscheidung. In der Praxis ebenfalls sehr wichtig ist der im BDSG geltende Zweckbindungsgrundsatz, der besagt, dass personenbezogene Daten nur für die zuvor konkret festgelegten und gesetzlich erlaubten Zwecke erhoben und verwendet werden dürfen. Im Ergebnis wird eine Totalüberwachung und damit Vollkontrolle der Internetnutzung und Kommunikation von Arbeitnehmern unverhältnismäßig und damit datenschutzrechtlich unzulässig sein. Zulässig, da verhältnismäßig kann dagegen eine stichprobenhafte und zeitnahe Auswertung der Protokolldaten des Arbeitnehmers sein.
„Wir empfehlen stets eine enge Abstimmung zwischen den internen Ermittlern und dem Datenschutzbeauftragten des Unternehmens und zuvor die Erstellung einer risikobasierten Analyse der konkreten einzelnen beabsichtigten Ermittlungsmaßnahmen, die insbesondere genau zu dokumentieren sind – und zwar sowohl im Vorfeld als auch im Zuge der Monitoring-Maßnahmen selbst", so Rechtsanwalt und Mediator Auffermann aus Berlin.
Der Forderung des IT-Experten und/oder Compliance-Beauftragten nach präventiven, permanenten Überwachungsmaßnahmen kann also nur äußerst selten gefolgt werden; die Unternehmensleitung muss Unwissenheit eher in Kauf nehmen als Datenschutzverstöße zu riskieren.

Ein Weg aus dem Dilemma führt über die Anonymisierung von Daten

Diesem Dilemma versuchen Anbieter von Datenreview- und E-Discovery-Lösungen zu begegnen. Eines der wesentlichen Charakteristika ist hierbei, die Datensammlung so vorzunehmen, dass die Einschränkungen des TKG und BDSG nicht zur Geltung kommen. Der Schlüssel hierfür ist die Anonymisierung beziehungsweise Pseudonymisierung personenbezogener Informationen: Datensätze werden so aufbereitet, dass von den gespeicherten Network-Datenpaketen die Informationen, die auf Personen Rückschlüsse zulassen würden, entfernt werden. Daten können so problemlos geprüft werden. Erhärtet sich ein Anfangsverdacht, kann die weitere Prüfung rechtmäßig durchgeführt werden, ergeben sich keine Verdachtsmomente, wird der Vorgang ohne Verletzung der relevanten Datenschutzvorgaben geschlossen werden. Ein Verfahren, das datenschutzrechtlich nicht zu beanstanden ist, wie Lukas Mempel erläutert: Ein Datenabgleich zur Überprüfung und dem Ausschluss dolosen Handelns sei grundsätzlich nicht unzulässig, solange alle Daten, die nicht relevant sind, „sozusagen geräuschlos aussortiert werden. Wenn ich am Ende nur die Daten erfasst habe, bei denen ein begründeter Anfangsverdacht besteht, kann ein solcher Datenabgleich in Ordnung sein."
Neben Datenschutz- und Telekommunikationsrecht spielen im Kontext von Monitoring auch arbeitsrechtliche Bestimmungen eine wichtige Rolle. So ist gemäß Betriebsverfassungsgesetz die Zustimmung des Betriebsrats bei Einrichtung von Monitoring- und Filterungsmaßnahmen erforderlich, weil diese potenziell zur Überwachung der Mitarbeiter eingesetzt werden und damit einen Personenbezug (datenschutzrechtlich spricht man von personenbezogenen oder personenbeziehbaren Daten) herstellen können.
Bei Krankenhäusern, die als Anstalten des öffentlichen Rechts organisiert sind, ist der Personalrat zuständig. Das Universitätsklinikum Heidelberg bereitet derzeit eine Dienstvereinbarung vor, die in bestimmten Fällen in einem mit dem Gesamtpersonalrat und dem Datenschutzbeauftragten eng abgestimmten Verfahren den Einsatz eines „Security Monitors" und die Protokollierung des Zugriffs von Beschäftigten auf den „Patientenorganizer" (elektronische Patientenakte) zulässt. „Damit sollen unrechtmäßige Zugriffe und Datenmissbrauch im Sinne von Datengeheimnis

und Schweigepflicht festgestellt und verfolgt werden können. Der Datenschutz für Patienten soll gestärkt werden“, so Dr. Christiane Tödter aus der Rechtsabteilung der Uniklinik. Die Dienstvereinbarung berücksichtige den datenschutzrechtlichen Grundsatz der Datensparsamkeit, die Protokollierung werde auf das notwendige Maß beschränkt. Generell berücksichtige das Universitätsklinikum daneben das Prinzip der minimalen Berechtigung bei der Vergabe von Zugangsberechtigungen: „Es dürfen nur die Berechtigungen erteilt und nur die Daten verarbeitet und genutzt werden, die für den Aufgabenbereich erforderlich sind“, erläutert Tödter.

Ob solche Betriebsvereinbarungen zukünftig möglicherweise obsolet werden oder aber stärker denn je erforderlich, wird auch davon abhängen, welche neuen Gesetze erlassen werden. Dem Richtlinien-Entwurf der Europäischen Kommission folgend, legte dieses Jahr das Bundesinnenministerium einen Gesetzesentwurf für die Erhöhung der Sicherheit informationstechnischer Systeme vor, der umfassende Meldepflichten vorsieht. Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) erließ ein Rundschreiben zu den Mindestanforderungen im Risikomanagement bei Kredit- und Finanzdienstleistungsinstitutionen, das ebenfalls eine umfassende Überwachung vorsieht. Auf der anderen Seite ist offen, wie die infrage stehende EU-Datenschutz-Grundverordnung das deutsche Datenschutzrecht beeinflussen wird.

Interview mit Lukas Mempel, Sana Kliniken AG, unter
unternehmensjurist.net/136monitor

Laut Vodafone-Datenschutzbeauftragtem und Legal Counsel Dr. Dirk Herkströter, werde es bei den Änderungen insbesondere um folgende Punkte gehen: eine Ausdehnung des Geltungsbereichs auf Datenverarbeitungstatbestände jedes Unternehmens, unabhängig von seinem Unternehmenssitz (damit wären dann auch Vergehen von US-Giganten wie Google, Facebook et cetera besser zu ahnden), eine Präzisierung von Datenlöschungsansprüchen (der provokante Begriff „right to be forgotten“ wird nicht mehr verwendet), die Möglichkeit des Kunden, einer Profilbildung anhand seiner Daten zu widersprechen und die Verpflichtung der Unternehmen, ein Risikomanagement aufzubauen, um Gefährdungstatbestände für Kundendaten frühestmöglich zu erkennen und durch Gestaltung der Dienste zu vermeiden.

Aber, alles in allem, werde es in puncto Datenschutz keine allzu großen Änderungen zur bisherigen Rechtslage geben, da in Deutschland schon jetzt Prinzipien wie Datenvermeidung und Datensparsamkeit, eine strikte Zweckbindung der Daten sowie Auskunfts-, Berichtigungs- und Löschungsansprüche von Kunden im Datenschutzrecht verankert sind, so Dirk Herkströter. Von daher wird auch die Gemengelage unter den Akteuren IT, Compliance und Datenschutz weiterhin eine spannende, aber nicht unmögliche Herausforderung im Unternehmensalltag bleiben.

Claudia Bonacker