Verhaltensregeln im IT-Bereich

Neben Datenschutzrecht, Urheber- und Softwarerecht war IT-Compliance ein Schwerpunktthema beim 7. Österreichischen IT-Rechtstag des Vereins Infolaw am 23. und 24. Mai 2013 in Wien.

Compliance steht für die Einhaltung von Gesetzen und Richtlinien in Unternehmen. Durch Abwehr von Fehlverhalten soll Schaden verhindert werden“, sagte Rechtsanwältin Dr. Sonja Dürager *(bpv Hügel Rechtsanwälte OG)* bei der dritten Session des IT-Rechtstages, in der Rechtsprobleme bei der Umsetzung von Compliance-Regelungen in einer Organisation behandelt wurden. Die „Pflicht zur Compliance“ beginnt mit der Erstellung eines Verhaltenskodexes. Sie trifft die für das Unternehmen nach außen hin Verantwortlichen, etwa den Geschäftsführer einer GmbH (§ 25 GmbH-Gesetz) oder den Vorstand einer Aktiengesellschaft (§ 84 Aktiengesetz). Vornehmlich im IT-Bereich wird das Interesse des Unternehmens an Vorbeugung, Aufklärung und Verfolgung illegitimer Verhaltensweisen mit dem Interesse der Betroffenen am Recht auf Privatleben, Geheimnisschutz und informationeller Selbstbestimmung kollidieren und zu einer Interessenabwägung führen.

Zur Gestaltung einer „Policy“ oder Betriebsvereinbarung zur privaten IKT-Nutzung durch Mitarbeiter hat Dürager auf die Regelungen des Beamtendienstrechtsgesetzes (§§ 79c – 79h BDG) als Beispiel hingewiesen. Grundsätzlich darf danach die IKT-Infrastruktur nur für dienstliche Zwecke eingesetzt werden.

In einem eingeschränkten Ausmaß ist auch die private Nutzung der für den Dienstbetrieb zur Verfügung stehenden Infrastruktur erlaubt, sofern sie nicht missbräuchlich erfolgt, dem Ansehen des öffentlichen Dienstes nicht schadet, der Aufrechterhaltung eines geordneten Dienstbetriebes nicht entgegensteht und sie die Sicherheit und Leistungsfähigkeit der IKT-Infrastruktur nicht gefährdet (§ 79d BDG).

Rechtsanwältin Sonja Dürager: „Die Pflicht zur Compliance beginnt mit der Erstellung eines Verhaltenskodexes.“

Rechtsanwalt Roland Marko: „Es gibt keine Verpflichtung, dass ein Arbeitnehmer privat Betriebsmittel zur Verfügung stellen muss.“

Zu Kontrollzwecken dürfen personenbezogene Daten der IKT-Nutzung nur verwendet werden, wenn dies zur Abwehr von Schäden an der IKT-Infrastruktur oder zur Gewährleistung ihrer korrekten Funktionsfähigkeit oder bei Verdacht einer gröblichen Dienstpflichtverletzung oder zum Zweck der Klarstellung des Sachverhalts erfolgt (§ 79e Abs. 2 BDG). Zur Wahrung der Verhältnismäßigkeit hat sich das im BDG ebenfalls zum Ausdruck gekommene Prinzip der „stufenweisen Kontrollverdichtung“ herausgebildet. Zunächst erfolgt eine anonymisierte Verarbeitung unter Verwendung statistischer Informationen zur Sicherstellung der Funktionalität des Systems, ohne dass noch der Verdacht eines Fehlverhaltens gegen eine bestimmte Person vorliegt. In einer zweiten Stufe werden statistische Daten mit einem einer bestimmten Person zuordenbaren Code verbunden (pseudonymisierte Verarbeitung); es besteht bereits die Vermutung eines Fehlverhaltens. In der dritten Stufe, wenn ein konkreter Verdacht gegen eine bestimmte Person besteht, werden Verkehrs- und letztlich Inhaltsdaten personenbezogen ausgewertet und der User wird identifiziert.

Whistleblowing ist ein vorgezeichneter Prozess zur vertraulichen Meldung mutmaßlicher Missstände. Die Einrichtung einer „Whistleblower-Hotline“ unterliegt der Vorabkontrolle durch die Datenschutzkommission (§ 18 Abs. 2 Z 2 DSG), da personenbezogene Daten über den Verdacht der Begehung von Straftaten (§ 8 Abs. 4 Datenschutzgesetz) übermittelt und verarbeitet werden.

Die Zulässigkeit der Verarbeitung ergibt sich aus der Pflicht des Arbeitgebers, rechtswidriges Verhalten festzustellen; aus der Corporate Governance, dem Ordnungsrahmen für die Leitung und Überwachung von Unternehmen; oder aus Verpflichtungen gegenüber der Konzerngesellschaft. Die Übermittlung von Daten an diese findet ihre Rechtfertigung in rechtlichen Verpflichtungen wie etwa dem *Sarbane-Oxley Act (SOX)*. In der Meldung an die DSK wird anzuführen sein, wer (Reduktion des Kreises der Betroffenen) und was (Relevanz der Verstöße) gemeldet werden darf und weshalb gemeldet werden soll. Zu beachten wird ferner sein, dass die Vertraulichkeit hinsichtlich der Identität des Hinweisgebers, außer bei bewusst falsch erhobenen Anschuldigungen, gewahrt

INFOLAW

IT-Rechtstag

Der seit dem Jahr 2003 bestehende gemeinnützige Verein „Infolaw – Forschungsverein für Informationsrecht und Immaterialgüterrecht“ mit Sitz in Wien veranstaltet wissenschaftliche Fachveranstaltungen, wie etwa den „Österreichischen IT-Rechtstag“, führt Forschungsprojekte durch und erstellt Rechtsgutachten.

Der Schwerpunkt der Vereinstätigkeit liegt auf E-Commerce-Recht, IT-Recht sowie Wettbewerbs- und Immaterialgüterrecht.

www.infolaw.at
www.it-rechtstag.at

FOTOS: KURT HICKISCH

IT-Rechtstag 2013: Schwerpunkt IT-Compliance.

bleibt, der Beschuldigte Zugang zu den Anschuldigungen (nicht zur Person des Hinweisgebers) erhält und die Mitarbeiter geschult werden. Ferner wird die Zustimmung des Betriebsrates (§§ 96, 96a ArbVG) bzw. der Mitarbeiter (§ 10 AVRAG) vorliegen müssen.

Dürager berichtete auch über das Ergebnis einer Befragung im Auftrag der Kanzlei *bpv Hügel Rechtsanwälte,* ob bei österreichischen Unternehmen ein Trend zur Einführung von Whistleblowing-Hotlines besteht. Demnach sind vor allem in Unternehmen, die in einem Konzernverbund stehen, derartige Systeme eingeführt. Etwa die Hälfte der bezeichneten Unternehmen verfügt weder über eine Compliance-Organisation, noch wurde ein Ethik-Kodex eingeführt. Eine Definition und Abgrenzung hat David Krebs *(Compliance Counsel GE Healthcare,* Stockholm) zur praktischen Umsetzung von Compliance Management verwendet: „Ethics" bedeutet „doing the right thing"; „Compliance" bedeutet „doing things right". Laut Krebs komme der Missbrauch von Whistleblowing relativ selten vor.

Forensik. Wie bei einer forensischen Untersuchung von Datenmaterial vorgegangen wird, schilderten Mag. Karin Mair und Lukas Reiter, MSc, von *Deloitte Financial Advisory GmbH*. Es geht etwa bei der Aufdeckung von Korruption um die Darstellung von Zahlungsströmen. Bei einem ersten Treffen mit dem Auftraggeber wird festgelegt, wonach gesucht werden soll, welche Datenbestände (E-Mails, Memos, Briefe, Kalkulationen u. a.) es gibt und wo diese gespeichert sind (Server, Computer, Festplatten, DVDs, Handys). Spezielle Tools ermöglichen die Wiederherstellung gelöschter Dateien. Nach dem Kopieren der Datenträger werden die Daten verschlüsselt abgespeichert, signiert und mit Zeitstempel versehen. Die Durchsicht großer Datenmengen erfolgt nach bestimmten Suchkriterien.

Auf die einzuhaltenden rechtlichen Aspekte ging Mag. Roland Marko *(Wolf Theiss Rechtsanwälte GmbH)* ein. Die verfassungsgesetzlich gewährleisteten Grundrechte auf Datenschutz (§ 1 DSG) und auf Achtung des Privat- und Familienlebens (Art. 8 EMRK) sowie das Persönlichkeitsrecht nach § 16 ABGB müssten gegenüber dem Kontrollinteresse des Arbeitgebers abgewogen werden. Dieses könne an Schadenersatzansprüchen und Geldbußen bestehen, an der Abwehr weiterer Angriffe auf Compliance-Verstöße, an einer Beweissicherung sowie einer Wiederherstellung der Zuverlässigkeit. Im Zuge der

FOTO: KURT HICKISCH

erwähnten „Kontrollverdichtung“ könne letztlich im Verdachtsfall auf Korrespondenzdaten zurückgegriffen werden. Eine Zustimmung (§ 4 Z 14 DSG) des Betroffenen zu solchen Maßnahmen sei auf Grund des Abhängigkeitsverhältnisses problematisch und könne zudem widerrufen werden. Eine Trennung zwischen geschäftlicher und privater Korrespondenz sei anhand von Schlüsselwörtern realisierbar. Die den Auftraggeber treffende Pflicht, den Betroffenen zu informieren, ergebe sich weniger „aus Anlass“, als vielmehr „im Zuge“ von Ermittlungen (§ 24 Abs. 1 DSG).

Da der Forensiker personenbezogene Daten verarbeitet, treffen ihn die Verpflichtungen zu Datensicherheitsmaßnahmen nach § 14 Abs. 2 DSG. Die Rechtsgrundlagen für die Verarbeitung ergeben sich aus Zustimmung, überwiegendem Interesse des Arbeitgebers oder Verpflichtungen im Konzern. Nicht auf Dauer angelegte Kontrollmaßnahmen bedürfen nicht der Zustimmung des Betriebsrates, dieser muss aber informiert werden.

„Bring Your Own Device“. Über Probleme beim Einsatz eigener technischer IT-Geräte (Smartphones, Tablets, Laptops) für betriebliche Zwecke („Bring Your Own Device“) referierte DI Dr. Wolfgang Freund *(DLA Piper Weiss-Tessbach Rechtsanwälte GmbH)*. Der Trend dazu kommt von Arbeitnehmerseite. Mitarbeiter wollen ihre eigenen Geräte verwenden. Für Unternehmen ergibt sich vordergründig insofern eine Kostenersparnis, als Anschaffungskosten erspart werden, die Mitarbeiter mit den Geräten vertraut sind und kleinere Probleme selbst lösen können. Durch die Vermischung von beruflicher und privater Sphäre entstehen aber Risiken.

Forensische Untersuchung von Datenmaterial: Grundrechte auf Datenschutz und auf Achtung des Privat- und Familienlebens sowie das Persönlichkeitsrecht gegenüber dem Kontrollinteresse des Arbeitgebers müssen abgewogen werden.

Im Arbeitsrecht besteht keine Verpflichtung, dass ein Arbeitnehmer privat Betriebsmittel zur Verfügung stellen muss. Das ist Sache des Arbeitgebers. Aus einer konstanten betrieblichen Übung könnte sich ein Rechtsanspruch zum Einsatz privater Geräte verdichten. Es sollten Regelungen zur privaten Verwendung getroffen werden.

Wenn der Arbeitgeber dem Mitarbeiter für ein besseres Gerät eine Aufzahlung leistet, entsteht Miteigentum bzw. ein Rechtsanspruch auf Rückzahlung des aufgezahlten Betrages. Dem Arbeitnehmer steht ferner ein Ersatz der notwendigen und nützlichen Aufwendungen zu (§ 1014 ABGB), somit der laufenden Kosten bei betrieblicher Verwendung, oder etwa der Ersatz von Roaming-Gebühren bei Auslandsreisen. Zu regeln sind ferner, am besten in einer Betriebsvereinbarung, Ersatzansprüche bei Verlust oder Beschädigung des Geräts. Für ein Unternehmen ist es wichtig, die Möglichkeit der Abänderung und Widerrufbarkeit getroffener Regelungen vorzusehen. Nach Zivil- und Handelsrecht sind Aufbewahrungspflichten für geschäftliche Korrespondenz zu beachten, ebenso im Steuerrecht. Das gilt auch für E-Mails. Geheimhaltungsverpflichtungen müssen auch hinsichtlich der privaten Geräte durchgesetzt werden können (z. B. bei allfälliger Weitergabe des Handys im Familienkreis), ebenso Löschungsansprüche bei Beendigung des Dienstverhältnisses. Um betriebliche Compliance-Regelungen überprüfen zu können, müssen Regelungen zur Übergabe der Geräte getroffen werden.

Bei Verwendung personenbezogener Daten bleibt der Arbeitgeber im Sinne des Datenschutzgesetzes Auftraggeber und ist somit für die Einhaltung der Datensicherheitsbestimmungen (§ 14 DSG) verantwortlich. Ihn trifft auch die Verpflichtung, die Betroffenen zu verständigen, wenn ihnen durch unrechtmäßige Verwendung ihrer Daten Schaden droht (Data Breach Notification; § 24 Abs.2a DSG). Der Verlust des Handys muss dem Arbeitgeber gemeldet werden, worauf der Mitarbeiter hinzuweisen ist.

Urheberrechtlich sind Software-Lizenzen zu beachten, die mitunter nur für den privaten Gebrauch eingeräumt werden. Der Arbeitgeber haftet für Urheberrechtsverletzungen, wenn solche im Betrieb seines Unternehmens von einem Bediensteten oder Beauftragten begangen worden sind oder drohen (§§ 81, 88 UrhG).

Es gibt Tools, die im Notfall die Daten auf einem mobilen Gerät über Fernzugriff löschen. Erfolgt eine solche Löschung ohne Zustimmung des Mitarbeiters, kann sich hinsichtlich seiner Daten (etwa Musik, Fotos) strafrechtlich der Tatbestand der Datenbeschädigung (§ 126a StGB) oder der Störung der Funktionsfähigkeit eines Computersystems (§ 126b) ergeben. Auch diesbezüglich empfiehlt sich eine Vereinbarung mit dem Arbeitnehmer. *Kurt Hickisch*

FOTO: EGON WEISSHEIMER