Mobile Deviced Compliance: Nice to have oder must?

Mobile Devices wie Netbooks, PDAs oder Business Phones haben sich in der Geschäftswelt rasch verbreitet, sowohl in privaten Unternehmen wie auch in den Verwaltungen der Kantone und des Bundes. Der rasche, allgegenwärtige Zugriff auf E-Mails und andere elektronische Geschäftsdaten oder die Übermittlung unmittelbar vor Ort erhobener Daten erweist sich als unbestreitbarer Vorteil gegenüber stationären Systemen und ist heute kaum mehr aus der Berufswelt wegzudenken.

Dr. iur. Reto Fanger

Der Einsatz mobiler Systeme erfordert entsprechende umfassende Strategien im Sinne einer Compliance-Organisation, einer sog. «Mobile Deviced Compliance», zu deren Bestandteil Unternehmensrichtlinien über den konkreten Einsatz von mobilen Kommunikationsmitteln (sog. Mobile Devices Compliance) gehören. Dass die Etablierung einer solchen umfassenden Mobile Deviced Compliance im Unternehmensbereich und deren Einhaltung aber nicht selbstverständlich ist, beweist eine kürzlich publizierte Zeitungsmeldung im Zusammenhang mit dem iPhone-Hype:

«Auch bei den Bundesangestellten ist das iPhone ein Renner. 680 Mitarbeiter haben bei ihrem Arbeitgeber bereits eines bezogen, weil sie beruflich auf ein multifunktionales Mobiltelefon angewiesen sind. Die Nachfrage nach den praktischen und ästhetischen Geräten von Apple ist bei Bundesangestellten stark steigend. Doch jetzt ist Schluss: Das Eidgenössische Finanzdepartement (EFD) hat entschieden, dass ab sofort in der ganzen Bundesverwaltung bis auf Weiteres keine iPhones mehr bestellt und eingeführt werden dürfen. Das Bundesamt für Informatik wurde zudem explizit angewiesen, keine neuen Aufträge zur Synchronisierung von iPhones mit den EDV-Anlagen des Bundes anzunehmen. Das mobile Gerät von Apple kommt deshalb für all jene Bundesangestellten, die ein multifunktionales Handy für ihre Arbeit brauchen, nicht mehr in Frage. Bis auf Weiteres können Bundesangestellte nur noch Smartphones anderer Marken bestellen und mit der EDV des Bundes verbinden. Warum stoppt der Bund nur iPhones und nicht auch multifunktionale Mobiltelefone anderer Marken? Peter Fischer, Delegierter für die Informatikstrategie des Bundes und damit höchster Informatiker der Bundesverwaltung, holt etwas umständlich aus: **Es gebe in der Bundesverwaltung Vorgaben zum Einsatz von multifunktionalen Mobiltelefonen. Diese erlauben laut Fischer den Einsatz von iPhones eigentlich nicht. Dennoch habe der Bund in letzter Zeit einigen Bundesangestellten iPhones abgegeben und für diese auch eine Synchronisation mit der Infrastruktur des Bundes zugelassen.** Der Bundesrat werde im Herbst entscheiden, welche Bedingungen für den Einsatz von multifunktionalen Handys in Zukunft für Bundesangestellte gelten. Weil noch nicht klar sei, wie dieser entscheidet, würden jetzt nur noch Smartphones abgegeben, die den heutigen Vorgaben des Bundes entsprechen.» («Berner Zeitung»/«Tages Anzeiger», 14.07.2010; Hervorhebungen durch den Verfasser).

Interessant an dieser Meldung sind im Compliance-Kontext nicht Gerätekategorie und Marke des eingesetzten Mobile Devices oder der Sinngehalt des verordneten Stopps, sondern der Umstand, dass in der Bundesverwaltung offenbar eine bestehende Mobile Devices Compliance seit einiger Zeit nicht mehr eingehalten wurde und darüber hinaus eine umfassende Strategie im Sinne einer Mobile Deviced Compliance offenbar nicht besteht. Daneben setzen viele private Betriebe, vorwiegend aus dem KMU-Sektor, Mobile Devices ein, ohne überhaupt eine Mobile Devices Compliance geschweige denn eine umfassende unternehmensspezifische Mobile Deviced Compliance-Struktur etabliert zu haben.

Verlangt die geforderte Mobile Deviced Compliance den Unternehmen und Verwaltungen übermässige Vorkehren ab, erscheint doch deren Festsetzung und Einhaltung als schwierig zu verwirklichen? Um dies zu beantworten, müssen zunächst die Begriffe geklärt werden:

Compliance bezeichnet die Gesamtheit aller zumutbaren Massnahmen, die das regelkonforme Verhalten eines Unternehmens, seiner Organisationsmitglieder und seiner Mitarbeiter im Hinblick auf alle gesetzlichen Gebote und Verbote sowie unternehmensinterne und vertragliche Regelungen begründen. Deren Umsetzung ist als dauerhafter Prozess und nicht als kurzfristige Massnahme zu verstehen. Compliance hat einen wirtschaftlichen Nutzen für die Unternehmen und deren Eigentümer, indem Kosten insbesondere durch Schäden, Strafzahlungen, notwendige Massnahmen oder Imageschäden vermieden werden sollen. Die Unternehmensleitung ist verpflichtet, alle notwendigen Massnahmen zu veranlassen. Im Falle eines Verstosses gegen diese Pflicht kann das Management für einen Verstoss gegen die Organisationssicher-

heit durch unzureichende Compliance-Organisation persönlich haftbar gemacht werden. IT-Compliance umfasst die Unternehmensführung unter Einhaltung der einschlägigen Regelungen im Bereich der IT-Landschaft und in Bezug auf die Anforderungen der IT-Systeme eines Unternehmens. Dazu gehören zur Hauptsache die Bereiche Informationssicherheit, Verfügbarkeit, Datenaufbewahrung und Datenschutz. Dementsprechend umfasst die Mobile Deviced Compliance als Teilbereich der IT-Compliance in umfassender Weise sämtliche Compliance-Anforderungen, die aus dem Einsatz von Mobile Devices im Unternehmen zu beachten sind.

Wie kann nun ein solch umfassendes System einer Mobile Deviced Compliance geschaffen werden? Mit der Einhaltung folgender vier Säulen lässt sich eine solche Struktur verwirklichen und auch dauerhaft betreiben:

1. Säule: Identifikation von Risiken

- Vergleich des Einsatzes von Mobile Devices mittels systematischer und kontinuierlicher Prozesse, im Hinblick auf die Produkte, Dienstleistungen und Prozesse im eigenen Unternehmen sowie mit denen in fremden Unternehmen in qualitativer und/oder quantitativer Hinsicht zu vergleichen (Benchmarking).
- Identifizierung und Analyse der rechtlichen Risiken des Einsatzes von Mobile Devices. Dies erfordert vorab Kenntnisse der entsprechenden rechtlichen Rahmenbedingungen.

2. Säule: Schaffung eines internen Informationssystems

- Einschätzung des unternehmensinternen Schulungsbedarfs.
- Entwicklung von Unternehmensrichtlinien für den Einsatz der mobilen Systeme (Mobile Devices Compliance) und kontinuierliche Anpassung bestehender Richtlinien.

3. Säule: Schaffung eines internen und externen Kommunikationssystems

- Schaffung eines unternehmensinternen Meldesystems für Verstösse gegen die Mobile Devices Compliance (Unternehmensrichtlinien).
- Entwicklung unternehmensinterner Verfahrensabläufe bei Beschwerden im Hinblick auf den Einsatz von Mobile Devices.
- Sicherstellung von Kontakten mit den zuständigen Behörden und Festlegung von Vorgehensweisen bei allfälligen Beschwerden über den Einsatz von Mobile Devices.

4. Säule: Schaffung eines internen Kontrollsystems

- Berufung eines Compliance-Beauftragten pro Unternehmensbereich: Der Einsatz von Mobile Devices fällt in die Zuständigkeit des IT-Compliance-Beauftragten.
- Entwicklung von Kontrollverfahren und internen Kommunikationsabläufen.

Mit der sorgfältigen, kritischen und dauerhaften Umsetzung dieser vier Säulen kann die Etablierung einer umfassenden Mobile Deviced Compliance-Struktur gewährleistet werden, die für den Einsatz von Mobile Devices unabdingbar ist, unabhängig ob deren Einsatz in privaten Unternehmen oder staatlichen Verwaltungen erfolgt. ■