Bring Your Own Device (BYOD) oder Corporate Owned, Personally Enabled (COPE): Bringt es das wirklich?

Unabhängig davon, ob Unternehmen ihren Mitarbeitenden erlauben, private mobile Endgeräte wie Smartphones, Tablets oder Laptops im Arbeitsbereich einzusetzen, oder ob sie konzerneigene Devices für die private Nutzung freigeben: Beide Modelle weisen Sicherheitsrisiken sowie arbeits- und datenschutzrechtliche Fragen auf. Der nutzbringende Einsatz von BYOD oder COPE für alle Beteiligten bedingt daher die Umsetzung zahlreicher einschlägiger rechtlicher, technischer und organisatorischer Massnahmen.

Von Dr. iur. Reto Fanger, Rechtsanwalt

Während die Arbeitnehmer bei BYOD mit ihren eigenen, nur teilweise kontrollierbaren mobilen Geräten auf das IT-Netzwerk des Arbeitgebers zugreifen, dürfen sie im COPE-Modell oftmals die mobilen Endgeräte des Unternehmens auch für private Zwecke einsetzen.

Beide Alternativen zum klassischen IT-Bereitstellungmodell bedürfen einer sorgfältigen Klärung der Sicherheitsrisiken sowie der arbeits- und datenschutzrechtlichen Fragen, um jeweils rechtzeitig die angemessenen rechtlichen, technischen und organisatorischen Massnahmen im Hinblick auf Entscheid, Umsetzung und Betrieb einer solchen Lösung treffen zu können.

Bring Your Own Device (BYOD): Bei BYOD handelt es sich um ein Modell, bei dem private mobile Endgeräte der Nutzer wie Smartphones, Tablets und/oder Laptops in die Netzwerke von Unternehmen oder Bildungseinrichtungen integriert werden. Die Nutzer verwenden bei diesem Modell ihre eigenen Geräte, allenfalls unterstützt durch einen Mitfinanzierungsbeitrag der Organisation.

Corporate Owned, Personally Enabled (COPE): Das COPE-Modell zeichnet sich dadurch aus, dass ein Unternehmen seine Angestellten mit mobilen Arbeitsgeräten wie Smartphones, Tablets und/oder Laptops ausstattet und diese auch für den privaten Gebrauch ausserhalb der Arbeitszeit freigibt. Das Unternehmen ist verantwortlich für die Bereitstellung der Dienste, weshalb es die Kontrolle über die berücksichtigten Hersteller, Modelle und Datentarife hat. COPE gilt sowohl als Gegensatz zum klassischen Bereitstellungsmodell der IT, bei dem ein Gerät zugewiesen wird, das stets am Arbeitsplatz bleibt, wie auch als Gegensatz zum BYOD-Modell.

Sicherheitsrisiken für Betriebs- und Geschäftsgeheimnisse sowie Personendaten

Beide Modelle setzen das Unternehmensnetzwerk und die Unternehmensdaten privaten Inhalten und Applikationen und somit auch privat verursachten Sicherheitsproblemen wie Malware, Viren oder Trojanern aus.

Dementsprechend müssen aus Unternehmenssicht sowohl Betriebs- und Geschäftsgeheimnisse wie auch Personendaten von Kunden sowie Mitarbeitenden geschützt werden, indem verschiedene rechtliche, technische und organisatorische Massnahmen (TOM) umgesetzt werden: Dazu gehören unter anderem eine Genehmigungspflicht durch bezeichnete Verantwortliche, Nutzungsweisungen für Mitarbeitende und Regelungen des Zugriffs zur Geräteüberprüfung, für Fernwartung oder zur Datenlöschung per MDM- oder EMM-Lösungen, die Verwendung eines Virtual Private Networks (VPN) oder anderer gesicherter Lösungen für den Datentransfer, die Implementierung von Firewalls, Sandboxes, Festplattenverschlüsselung, Webmail sowie die Einführung von strengen Passwort-Policies oder die Regelung der geschäftlichen Datenablage, die nicht auf dem mobilen Endgerät, sondern auf einem lokalen Unternehmensserver oder einer Unternehmenscloud erfolgen soll.

Mobile Device Management (MDM): Die zentralisierte Verwaltung von Mobilgeräten durch Administratoren mithilfe von Soft- sowie Hardware umfasst die Inventarisierung der mobilen Geräte in Organisationen, die Software-, Daten- und Richtlinienverteilung sowie den Schutz der Daten auf diesen Geräten.

Enterprise Mobility Management (EMM): Zentrale Verwaltungsplattform für den sicheren und wirtschaftlichen Betrieb von Mobilgeräten in Unternehmen und deren Einbindung ins Unternehmensnetzwerk, bestehend aus Mobile Device Management (MDM), Mobile Application Management (MAM) und Mobile Content Management (MCM).

Arbeitsrechtliche Aspekte

Neben der risikobehafteten Sicherheit gibt es auch zahlreiche arbeitsrechtliche Fragen, die ein Unternehmen mit dem BYOD- oder COPE-Modell zu klären hat, wie beispielsweise die Ar-

beitszeitkontrolle, ständige Verfügbarkeit (Work-Life-Balance), Nutzung von Lizenzen oder Haftungsfragen.

Zudem muss sich ein Unternehmen die Frage stellen, wie diese mobilen Endgeräte technisch kontrolliert und allenfalls überwacht werden können, sei dies im Rahmen der eingesetzten MDM- oder EMM-Lösung oder mit anderen Überwachungstools.

Die Rechtsgrundlagen

Dies aber immer vor dem Hintergrund, dass nach Art. 26 ArGV 3 lediglich eine stichprobenweise Randdatenauswertung des E-Mail- und Internetverkehrs des Arbeitnehmers zulässig ist und eine Auswertung privater Inhalte bloss unter Einhaltung der einschlägigen strafrechtlichen Anforderungen von Art. 179bis und 179^{quinquies} StGB möglich wäre. Beides gilt jeweils unter gleichzeitiger Beachtung datenschutzrechtlicher Prinzipien wie der Verhältnismässigkeit, Zweckbindung und Transparenz, was schliesslich eine erhebliche Einschränkung der Kontrolle durch das Unternehmen zur Folge hat.

Die entsprechenden Entscheide finden Eingang in einschlägige Regelungen in den Nutzungsweisungen für Mitarbeitende sowie die Weisungen zur Regelung des Zugriffs zur Geräteüberprüfung, für Fernwartung oder zur Datenlöschung.

Datenschutzrechtliche Aspekte

Problembehaftet aus arbeits- sowie datenschutzrechtlicher Sicht ist nicht nur eine systematische MDM- oder EMM-basierte Kontrolle der mobilen Endgeräte, sondern bereits der blosse Zugriff auf die Geräte durch das Unternehmen im Einzelfall: Sowohl bei BYOD wie auch bei COPE ist problematisch, dass die persönlichen Daten des Arbeitnehmers, die auf dem mobilen Endgerät bearbeitet werden, nicht von der geschäftlichen Datenbearbeitung und den entsprechenden Unternehmensdaten getrennt sind.

Ausschlus des Zugriffs Unberechtigter

Bei Zugriff des Arbeitgebers auf die Geschäftsdaten kann daher der gleichzeitige Zugriff auf die privaten Arbeitnehmerdaten ohne aufwendige technische und organisatorische Massnahmen nicht ausgeschlossen werden. Gleiches gilt für Dritte, beispielsweise Familienangehörige des Arbeitnehmers, die zumindest bei BYOD diese mobilen Endgeräte ebenfalls mitbenutzen, während dies im COPE-Modell durch die Unternehmen in der Regel durch entsprechende Benutzerweisungen generell ausgeschlossen sein dürfte.

Aus datenschutzrechtlicher Sicht unabdingbar sind daher – abgesehen von der generellen Gewährleistung der Datensicherheit – die technische und logische Trennung von geschäftlichen und privaten Daten, die Einführung von entsprechenden spezifizierten Nutzungsweisungen für Mitarbeitende sowie die umfassende Regelung des Zugriffs zur Geräteüberprüfung, für Fernwartung oder zur Datenlöschung inklusive transparenter vorgängiger Information der Mitarbeitenden.

Rechtliche, technische und organisatorische Massnahmen bei BYOD/COPE

Zusammenfassend sind unternehmensseitig zur Risikobegrenzung sowie für die rechtskonforme Umsetzung und den Betrieb sowohl von BYOD- wie COPE-Modellen folgende Massnahmen zu implementieren und stets dem jeweils aktuellen technischen Stand anzupassen:

- Genehmigungspflicht durch bezeichnete Verantwortliche
- transparente Nutzungsweisungen für Mitarbeitende
- transparente Regelung des Zugriffs zur Geräteüberprüfung, für Fernwartung oder zur Datenlöschung per MDM- oder EMM-Lösungen
- Trennung von geschäftlichen und privaten Daten (technisch und logisch)
- technische und organisatorische Massnahmen (TOM) wie VPN oder andere sichere Übertragungskanäle, Firewalls, Sandboxes, Festplattenverschlüsselung, Webmail, Passwort-Policies etc.
- Regelung der geschäftlichen Datenablage auf lokalem Unternehmensserver oder einer Unternehmenscloud

AUTOR

Dr. iur. Reto Fanger ist Rechtsanwalt (ADVOKATUR FANGER – Anwaltsboutique für ICT-, Daten-, Medien- & Arbeitsrecht, Luzern; www.advokatur-fanger.ch), Dozent an der Hochschule Luzern und Mitorganisator des Lucerne Law & IT Summit (LITS) der Uni Luzern.