BYOD im Arbeitsrecht: Chancen, Risiken und Regelungsbedarf

Die zunehmende Digitalisierung der Arbeitswelt, mobile Arbeitsformen und insbesondere die Verbreitung von Homeoffice haben dazu geführt, dass die Arbeit längst nicht mehr nur am festen Arbeitsplatz mit vom Arbeitgebenden bereitgestellter Infrastruktur verrichtet wird. Unter «Bring Your Own Device» **(«BYOD»)** wird die Nutzung privater Geräte wie Smartphones, Tablets oder Laptops zu geschäftlichen Zwecken verstanden.

■ **Von Dr. iur. Stefan Eichenberger und Tim Vetterli**



Arbeitsrechtlich stellen sich dabei insbesondere Fragen zur Bereitstellung und Finanzierung der Arbeitsgeräte sowie zum Datenschutz, zur Datensicherheit, zur Arbeitszeit und zur Haftung. Diese Schnittstellen zwischen Arbeitsrecht, Datenschutzrecht und IT-Sicherheit gilt es für Arbeitgebende präventiv und rechtssicher zu regeln.

Allgemeine gesetzliche Grundlagen

Grundsätzlich haben Arbeitgebende gemäss Art. 327 Abs. 1 OR die für die Arbeit erforderlichen Geräte und Materialien zur Verfügung zu stellen. Setzt der Arbeitnehmende mit Zustimmung des Arbeitgebenden eigene Arbeitsmittel ein, ist er nach Art. 327 Abs. 2 OR dafür angemessen zu entschädigen, sofern nichts anderes vereinbart oder üblich ist. Eine solche Abrede kann auch stillschweigend erfolgen. Eine entsprechende Übung besteht etwa bei Artisten oder bei Musikern hinsichtlich ihrer Instrumente. Eine entschädigungslose Übung ist bisweilen bei Köchen mit eigenen Messern oder im Coiffeurgewerbe mit eigenen Scheren verbreitet.

Der Entschädigungsanspruch setzt grundsätzlich das Einverständnis des Arbeitgebenden voraus. Höhe und Form der Entschädigung können vereinbart oder pauschal festgelegt werden; zu berücksichtigen sind insbesondere Umfang der geschäftlichen Nutzung, Abnutzung und Nutzungsdauer. Bei BYOD empfiehlt sich eine schriftliche Regelung.

Davon zu unterscheiden ist der zwingende Auslagenersatz nach Art. 327a OR, etwa für zusätzliche geschäftliche Daten-, Verbindungs- oder Roamingkosten. Eine Pauschale ist zulässig, sofern sie die notwendigen Auslagen im Durchschnitt deckt.

Wird ein primär privat angeschafftes Smartphone lediglich gelegentlich und freiwillig geschäftlich genutzt und stellt der Arbeitgebende eine zumutbare Alternative bereit, besteht grundsätzlich kein Anspruch auf Beteiligung am Anschaffungspreis. Verlangt oder akzeptiert der Arbeitgebende hingegen eine regelmässige geschäftliche Nutzung, können eine Nutzungsentschädigung und der Ersatz zusätzlicher Auslagen geschuldet sein. In der Praxis empfiehlt sich hier die Vereinbarung einer monatlichen (Spesen-)Pauschale.

Nutzung privater Arbeitsmittel

Arbeitgebende können die Nutzung von privaten Geräten erlauben. Das Modell kann freiwillig ausgestaltet oder vertraglich beziehungsweise durch einen GAV vorgeschrieben werden. Eine Verpflichtung, erhebliche private Anschaffungskosten zu übernehmen, sollte nicht bloss auf eine einseitige Weisung gestützt, sondern vertraglich so vereinbart werden.

Arbeitnehmende verfügen umgekehrt über keinen gesetzlichen Anspruch auf den Einsatz ihrer eigenen privaten Geräte. Der Arbeitgebende darf BYOD insbesondere aus Sicherheits-, Datenschutz-, Kompatibilitäts- oder Lizenzgründen einschränken oder gänzlich ausschliessen.

Chancen und Risiken

Auf der einen Seite kann BYOD Vorteile für beide Parteien bieten. Der Arbeitgebende kann von einem reduzierten Beschaffungsaufwand sowie tieferen direkten Gerätekosten profitieren. Die Arbeitnehmenden wiederum schätzen die freie Gerätewahl und die Nutzung vertrauter Hardware, was die Akzeptanz und Effizienz im Arbeitsalltag steigern kann. Zudem entfällt das lästige Mitführen eines zweiten geschäftlichen Geräts, was die Flexibilität im Homeoffice und auf Reisen erhöht.

Demgegenüber stehen jedoch gewichtige Risiken. Der administrative Aufwand für die IT-Abteilung kann durch die Vielfalt an Betriebssystemen und Gerätetypen ansteigen. Zudem besteht eine erhöhte Gefahr von Datenabflüssen durch mangelhafte Sicherheitsupdates, unsichere Apps, private Cloud-Back-ups,

Geräteverlust oder die unkontrollierte Nutzung des privaten Geräts im familiären Umfeld. Gleichzeitig kann sich die saubere Abgrenzung zwischen geschäftlichen Daten und der geschützten Privatsphäre des Arbeitnehmenden im Alltag als schwierig erweisen.

Datenschutz, Überwachung und Fürsorgepflicht

Verantwortung und IT-Sicherheit

Grundsätzlich liegt die Verantwortung zur Sicherstellung des Datenschutzes am Arbeitsplatz beim Arbeitgebenden. Er muss durch angemessene technische und organisatorische Massnahmen **(«TOM»)** eine dem Risiko entsprechende Datensicherheit gewährleisten. Dazu gehören je nach Schutzbedarf etwa Verschlüsselung, Mehrfaktor-Authentisierung **(«MFA»),** gesicherte Verbindungen **(«VPN»),** regelmässige Updates, Zugriffsbegrenzungen und ein geregelter Umgang mit Sicherheitsvorfällen.

Eine BYOD-Regelung sollte insbesondere die zugelassenen Geräte, Betriebssysteme, Updates, Verschlüsselung, erlaubte Apps, Speicherung, Back-ups, Support, Verlustmeldungen und das Vorgehen bei Sicherheitsvorfällen regeln. Geschäftliche Daten sind soweit möglich technisch von privaten Daten zu trennen, beispielsweise durch geschäftliches Container-, Mobile-Device-Management **(«MDM»)** oder virtuelle Desktop-Lösungen **(«VDI»).**

Persönlichkeitsschutz und Überwachung

Die Fürsorgepflicht nach Art. 328 OR, ergänzt durch Art. 328b OR, verpflichtet den Arbeitgebenden, die Persönlichkeit der Arbeitnehmenden zu schützen und Personendaten über sie nur zu bearbeiten, soweit diese ihre Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrags erforderlich sind. Kontrollen und technische Verwaltungsinstrumente müssen transparent, zweckgebunden und verhältnismässig sein. Systeme, die ausschliesslich oder hauptsächlich das Verhalten der Arbeitnehmenden überwachen, sind nach Art. 26 ArGV 3 unzulässig.

Hinsichtlich der Überwachung und des Zugriffs auf das private Gerät gelten enge gesetzliche Grenzen. Ein direkter Zugriff des Arbeitgebenden auf rein private Daten wie persönliche Nachrichten, Fotos oder Standortdaten ist grundsätzlich unzulässig. Um die erforderliche Transparenz zu wahren, müssen die Arbeitnehmenden vorab darüber informiert werden, welche Daten erhoben werden, welche Verwaltungsfunktionen des MDM aktiv sind und wer Zugriff darauf erhält.

Auch bei einer allfälligen Fernlöschung **(«Remote Wipe»)** im Verlustfall ist Vorsicht geboten; eine vollständige Löschung des privaten Geräts ist regelmässig unverhältnismässig und sollte vermieden werden. Vorzugswürdig ist die gezielte Löschung eines technisch abgegrenzten geschäftlichen Bereichs. Das Bundesgericht hat den unbefugten Zugriff eines Arbeitgebenden auf private Nachrichten eines Arbeitnehmenden als Persönlichkeitsverletzung beurteilt.

Pflichten bei Beendigung des Arbeitsverhältnisses

Beim Austritt sind geschäftliche Daten und Zugangsrechte kontrolliert vom privaten Gerät zu entfernen beziehungsweise zu sperren. Aufbewahrungspflichtige oder für den Geschäftsbetrieb benötigte Unterlagen sind vorgängig an den Arbeitgebenden zu übergeben oder in dessen Systemen zu sichern. Private Daten dürfen dabei grundsätzlich weder eingesehen noch gelöscht werden.

Mitwirkungspflicht der Arbeitnehmenden

Den Arbeitnehmenden kommt im Rahmen ihrer Sorgfalts- und Treuepflicht gemäss Art. 321a OR eine Mitwirkungspflicht bei Datenschutz und Datensicherheit zu. Sie haben zudem rechtmässige Weisungen gemäss Art. 321d OR zu befolgen. Dazu gehören insbesondere die Einhaltung der Sicherheitsvorgaben, der Schutz von Zugangsdaten und die unverzügliche Meldung von Verlust, Diebstahl oder Sicherheitsvorfällen. Der Arbeitgebende muss seinerseits geeignete Weisungen erlassen und die Mitarbeitenden angemessen informieren und schulen.

Arbeitszeit und Erreichbarkeit

Die Nutzung eines privaten Geräts begründet für sich allein keine Pflicht zur ständigen Erreichbarkeit. Wird das Lesen oder Beantworten geschäftlicher Nachrichten ausserhalb der üblichen Arbeitszeit angeordnet oder erkennbar erwartet, kann dies Arbeitszeit darstellen. BYOD-Regelungen sollten deshalb Erreichbarkeitsfenster, Reaktionszeiten, Zeiterfassung sowie den Umgang mit Nacht-, Sonntags- und Ruhezeiten festlegen. Die arbeitsgesetzlichen Vorgaben gelten unabhängig vom Arbeitsort.

Softwarelizenzen

Zur Nutzung einer Software wird der Erwerb entsprechender Lizenzen vorausgesetzt, wobei zwischen privaten und geschäftlichen Lizenzen zu unterscheiden ist. Ob eine auf einem privaten Gerät vorhandene Lizenz geschäftlich genutzt werden darf, richtet sich nach den jeweiligen Lizenzbedingungen. Privat-, Bildungs- oder App-Store-Lizenzen erlauben eine kommerzielle Nutzung nicht zwingend. Ebenso ist zu prüfen, ob die vom Unternehmen erworbenen Lizenzen die Installation auf privaten Geräten, Mehrfachinstallationen oder einen Fernzugriff abdecken.

Arbeitgebende sollten deshalb regeln, dass auf privaten Geräten nur vom Arbeitgebenden freigegebene und ordnungsgemäss lizenzierte Software für geschäftliche Zwecke verwendet werden darf, um Lizenzverletzungen, Sicherheitsrisiken und sogenannte Schatten-IT zu vermeiden.

Ein VPN schützt zwar die Verbindung zum Unternehmensnetz, löst aber nicht sämtliche Lizenz- und Sicherheitsfragen. Je nach System können virtuelle Desktops, browserbasierte Anwendungen oder geschäftliche Container verhindern, dass Daten lokal gespeichert oder nicht freigegebene Programme eingesetzt werden.

Haftung

Die Haftung bei Datenverlusten oder anderen Schäden lässt sich nicht pauschal dem Arbeitgebenden oder dem Arbeitnehmenden zuweisen. Gegenüber Kunden oder anderen Dritten hängt sie von der jeweiligen gesetzlichen oder vertraglichen Grundlage ab. Art. 55 OR (Geschäftsherrenhaftung des Arbeitgebenden) kann zur Anwendung gelangen, wenn ein Arbeitnehmender in Ausübung geschäftlicher Verrichtungen widerrechtlich einen Schaden verursacht. Daneben können vertragliche Haftungsgrundlagen und datenschutzrechtliche Verantwortlichkeiten bestehen.



Grafik generiert mit Napkin

Im Innenverhältnis ist der Arbeitnehmende nach Art. 321e OR für Schäden verantwortlich, die er dem Arbeitgebenden absichtlich oder fahrlässig zufügt. Das Mass der Sorgfalt bestimmt sich nach dem einzelnen Arbeitsverhältnis unter Berücksichtigung des Berufsrisikos, des Bildungsgrads sowie der Fachkenntnisse und Fähigkeiten des Arbeitnehmenden.

Häufig ist schwer nachzuweisen, ob ein Datenleck auf die Nutzung des privaten Geräts und eine Pflichtverletzung des Arbeitnehmenden zurückzuführen ist. Klare Vorgaben, Sicherheitsmassnahmen und Schulungen sind daher zentral.

Auch bei Diebstahl oder Beschädigung eines privaten Geräts haftet der Arbeitgebende nicht automatisch. Massgebend sind insbesondere Schadensursache, Verschulden, geschäftliche Nutzung, vertragliche Risikoverteilung und Versicherungsdeckung. Die BYOD-Vereinbarung sollte deshalb die Tragung von Reparatur-, Ersatz- und Wiederherstellungskosten regeln.

Exkurs: COPE

«Corporate owned, personally enabled» **(«COPE»)** bedeutet, dass der Arbeitgebende die Arbeitsgeräte zur Verfügung stellt, diese die Arbeitnehmenden jedoch auch für private Zwecke verwenden dürfen.

Das COPE-Modell kann als Mittelweg zwischen BYOD und dem klassischen Modell gesehen werden, bei dem der Arbeitgebende Geräte zur ausschliesslich geschäftlichen Verwendung zur Verfügung stellt. Der Arbeitgebende kann das Gerät einheitlich konfigurieren, absichern und verwalten. Sein Eigentum verschafft ihm jedoch keinen unbegrenzten Zugriff auf private Daten. Die zulässige private Nutzung, Kontrollen, Back-ups, Fernlöschung sowie die Trennung privater und geschäftlicher Inhalte müssen auch bei COPE transparent und verhältnismässig geregelt sein.

Die Beendigung des Arbeitsverhältnisses gestaltet sich grundsätzlich einfacher: Beim Austritt ist das Gerät dem Arbeitgebenden zurückzugeben. Den Arbeitnehmenden ist zuvor Gelegenheit zu geben, zulässige private Daten zu sichern und zu entfernen. Anschliessend können die geschäftlichen Daten zentral gesichert und das Gerät neu aufgesetzt werden.

Fazit

BYOD bietet Flexibilität, erhöht jedoch die Risiken insbesondere in den Bereichen Datenschutz, IT-Sicherheit, Kosten und Haftung. Die gesetzlichen und vertraglichen Pflichten des Arbeitgebenden bleiben bestehen.

Die Nutzung privater Geräte sollte deshalb nicht bloss geduldet, sondern in einer klaren BYOD-Regelung festgehalten werden. Diese sollte insbesondere Sicherheitsvorgaben, Kosten, Zugriffsrechte, Arbeitszeit, Haftung sowie das Vorgehen bei Verlust und Austritt regeln.

Als Alternative kann sich das COPE-Modell anbieten. Welches Modell geeignet ist, hängt von den betrieblichen Abläufen, den bearbeiteten Daten und dem erforderlichen Sicherheitsniveau ab.

AUTOREN



Dr. iur. Stefan Eichenberger ist Partner bei der EPARTNERS AG in Zürich. Er berät und unterstützt seine Klienten insbesondere in folgenden Tätigkeitsgebieten: Vertragsrecht (insbesondere Arbeitsrecht), Gesellschaftsrecht, Erbrecht, Datenschutzrecht sowie in der Prozessführung.



MLaw Tim Vetterli ist Rechtsanwalt bei der EPARTNERS AG in Zürich. Er ist schwerpunktmässig im Vertragsrecht (insbesondere Arbeitsrecht), im IT- und Technologierecht, Datenschutz- und Gesellschaftsrecht beratend als auch prozessierend tätig.