Zeitschrift für Datenrecht und Informationssicherheit

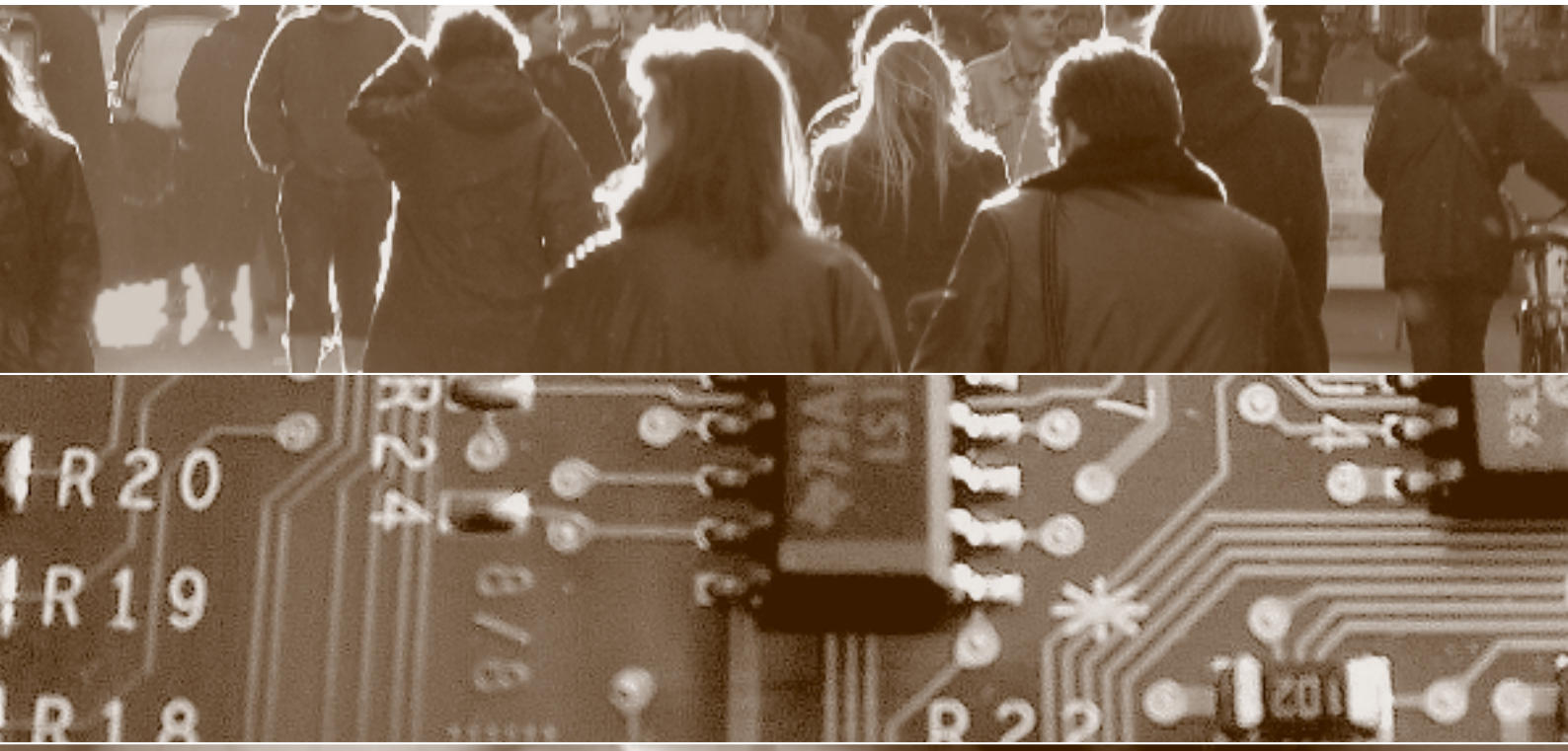
digma

www.digma.info 12. Jahrgang, Heft 4, Dezember 2012

Schwerpunkt:

Faktor Mensch

fokus: Informationssicherheitskultur
fokus: Rechtliche Stolpersteine bei «BYOD»
report: Datenschutzaufsicht über Spitäler



Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth

Schulthess §

fokus

Schwerpunkt:
Faktor Mensch

Informationssicherheitskultur

Nur befähigte, verantwortungsbewusste und loyale Mitarbeitende sind in der Lage, sich sicher zu verhalten. Mit einem gezielten Prozess kann erfolgreich eine geeignete Informationssicherheitskultur aufgebaut werden, die das ermöglicht. Wie kann eine solche Informationssicherheitskultur gemessen, geplant und gesteuert werden?

Loyalität im «Nomad Age»

Bei den Mitarbeitenden ein «Grundrauschen» zum Thema Informationssicherheit zu erreichen, ist keine grosse Herausforderung mehr. Doch welche Rolle kommt dabei den Führungskräften zu? Loyalität wird zum Motor für eine aktive und gelebte Sicherheitskultur.

Rechtliche Stolpersteine bei «BYOD»

«Bring Your Own Device» wirft verschiedene arbeits- und datenschutzrechtliche Fragen auf. Arbeitgeber, welche die Nutzung privater Geräte wie Laptops oder Smartphones zulassen, sollten vorgängig diese Fragen klar regeln.

Usable Security

IT-Sicherheits- und Privatsphäremechanismen sind nur effektiv, wenn sie vom Menschen verstanden und korrekt angewendet werden. Der Mensch muss deshalb als integraler Teil eines soziotechnischen Systems begriffen und in die Entwicklung von anwenderfreundlichen Sicherheitsmechanismen einbezogen werden.

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. Dr. iur. Rainer J. Schweizer, Dr. Günter Karjoth

Redaktion: Dr. iur. Bruno Baeriswyl und Dr. iur. Beat Rudin

Rubrikenredaktorin: Dr. iur. Sandra Husi-Stämpfli

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 131.00 (inkl. Versandspesen), Einzelheft: CHF 42.00

Anzeigenmarketing: Publicitas Publimag AG, Mürtschenstrasse 39, Postfach, CH-8010 Zürich
Tel. +41 (0)44 250 31 31, Fax +41 (0)44 250 31 32, www.publimag.ch, service.zh@publimag.ch

Herstellung: Schulthess Juristische Medien AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich
Tel. +41 (0)44 200 29 19, Fax +41 (0)44 200 29 08, www.schulthess.com, zs.verlag@schulthess.com

Rechtliche Stolpersteine bei «BYOD»

Arbeits- und datenschutzrechtliche Gedanken zum aktuellen Trend «Bring Your Own Device» (BYOD)

Mark A. Reutter, Dr. iur., Rechtsanwalt, Partner bei Walder Wyss AG, Zürich, Lehrbeauftragter an der Universität Freiburg
mark.reutter@walderwyss.com

Samuel Klaus, Dr. iur., Rechtsanwalt, Associate bei Walder Wyss AG, Zürich
samuel.klaus@walderwyss.com

Arbeitgeber, welche die Nutzung privater Geräte wie Laptops oder Smartphones zulassen, sollten vorgängig einige rechtliche Fragen klar regeln.

BYOD steht für «Bring Your Own Device». Es bezeichnet den aktuellen Trend, dass Unternehmen ihren Arbeitnehmern erlauben, private IT-Geräte (Laptop, Tablets, Smartphones etc.) zur Arbeitsleistung zu nutzen. Unternehmen setzen BYOD insbesondere zur Produktivitätssteigerung und Incentivierung technikaffiner Arbeitnehmer ein[1]. Letztere sind mit ihren privaten Geräten bereits vertraut, besser erreichbar und verfügen oft auch über leistungsfähigere Geräte, als sie vom Arbeitgeber sonst zur Verfügung gestellt werden.

Bring Your Own Device

Bei der Umsetzung von BYOD stellen sich Fragen auf betriebswirtschaftlicher, technischer und rechtlicher Ebene[2]. Technische und rechtliche Unterschiede ergeben sich vor allem im Vergleich zu den alternativen Konzepten «CYOD» (Choose Your Own Device) und «PUOCE» (Private Use of Company Equipment)[3]. Grundsätzlich stellen sich zwar auch bei CYOD und PUOCE ähnliche Fragen wie bei BYOD. Da aber die «Gerätehoheit» beim Arbeitgeber verbleibt, können diese auf einfachere Weise gelöst werden als bei BYOD, unter welchem die privaten Geräte der Arbeitnehmer eingesetzt werden.

Arbeitgeber, die sich für BYOD entscheiden, haben ein besonderes Augenmerk auf verschiedene arbeits- und datenschutzrechtliche Aspekte zu richten. Aber auch Arbeitgeber, die nicht auf BYOD setzen, sollten sich mit diesen Punkten auseinandersetzen. Der Einsatz privater Geräte durch Arbeitnehmer ist nämlich auch ohne explizite Regelung vielfach bereits Realität[4].

Arbeitsrecht

Übersicht

Das Obligationenrecht (OR)[5] enthält in Art. 319 ff. privatrechtliche Vorschriften zum Arbeitsverhältnis, die durch die öffentlich-rechtlichen Vorschriften des Arbeitsgesetzes (ArG)[6] und der zugehörigen Verordnungen[7] ergänzt werden. Bei BYOD sind vor allem folgende Themen näher zu betrachten:

- Zurverfügungstellung der Arbeitsmittel,
- Einführung von BYOD,
- Haftung bei Beschädigung/Verlust,
- Ausfallzeiten/Ersatzgeräte,
- Betrieb, Support und Unterhalt,
- Ferien-/Arbeitszeiten.

Zurverfügungstellung der Arbeitsmittel

Bei den von BYOD betroffenen Geräten handelt es sich um «Arbeitsmittel», mit denen die Arbeitnehmer ihre Arbeitsleistung erbringen. Arbeitsmittel sind gemäss Art. 327 OR vom Arbeitgeber zur Verfügung zu stellen. Die Parteien können aber eine abweichende Regelung vorsehen. Stellt der Arbeitnehmer die Arbeitsmittel, so ist er dafür grundsätzlich zu entschädigen, sofern die Parteien keine abweichende Regelung getroffen haben.[8]

Für BYOD kann somit vorgesehen werden, dass der Arbeitnehmer sein eigenes Gerät beschafft und die entsprechenden Kosten vollständig selbst trägt. Dies setzt aber eine explizite Regelung voraus.

Alternativ kann der Arbeitnehmer sein eigenes Gerät beschaffen, muss dafür aber gemäss Art. 327 Abs. 2 OR angemessen entschädigt werden. Voraussetzung hierfür ist nur, dass der Arbeitgeber mit der Verwendung eigener Geräte durch den Arbeitnehmer einverstanden ist. Ein solches Einverständnis ist auch stillschweigend möglich[9]. Ein Arbeitgeber, der ohne explizite Regelung toleriert, dass sein Arbeitnehmer private Geräte verwendet, läuft somit Gefahr, dass der Arbeitnehmer einen Entschädigungsanspruch nach Art. 327 Abs. 2 OR geltend macht. Eine «Usanz» in dem Sinne, was bezüglich Kostentragung üblich und angemessen ist, be-

steht zurzeit (noch) nicht. Es ist deshalb in allen Fällen eine klare Regelung empfehlenswert.

Selbstverständlich ist – auf freiwilliger Basis oder aufgrund entsprechender Regelung – auch eine vollständige Kostenübernahme durch den Arbeitgeber denkbar.

Einführung von BYOD

Bei der Einführung von BYOD ist zu unterscheiden, ob BYOD bloss als freiwillige und zusätzliche Option eingeführt wird oder als Pflicht der Arbeitnehmer (z.B. um die bisherige IT-Lösung gesamthaft zu ersetzen).

Wird BYOD als optionale Variante zusätzlich zur bisherigen IT-Lösung eingeführt, muss nur auf eine klare Regelung mit denjenigen Arbeitnehmern geachtet werden, die BYOD in Anspruch nehmen. Zu erwähnen sind hier auch die internen IT-Policies wie Benutzungsreglemente, Sicherheitsvorgaben, Regelung von Überwachung und Datenherausgabe etc., die insbesondere auch die jeweils nötigen Zustimmungserklärungen der Arbeitnehmer zu enthalten haben (vgl. dazu den Abschnitt «Datenschutz»).

Soll BYOD hingegen anstelle der bisherigen IT-Lösung treten, müssten alle Arbeitnehmer zu BYOD verpflichtet werden. Eine solche Änderung in einem laufenden Arbeitsverhältnis geht über das im Rahmen des Weisungsrechts (Art. 321d OR) Zulässige hinaus[10]. Entsprechend wäre eine Abänderung des Arbeitsvertrags nötig – und damit die Zustimmung beider Parteien. Schriftlichkeit ist zwar nur in bestimmten Fällen vorgeschrieben (Art. 320 Abs. 1, 327a Abs. 2 OR), aber nur schon aus Beweisgründen in jedem Fall ratsam. Versucht ein Arbeitgeber, Vertragsänderungen unter Kündigungsandrohung durchzusetzen, stellt sich die Frage nach der Zulässigkeit von Änderungskündigungen[11].

Festzuhalten ist, dass BYOD auch durch die Arbeitnehmer nicht etwa einseitig «eingeführt» werden kann, sondern nur mit Einverständnis des Arbeitgebers. Dieses kann aber auch stillschweigend durch Duldung der Nutzung privater Geräte erteilt werden, was bereits zu einer Entschädigungspflicht des Arbeitgebers führen kann (vgl. vorgängigen Abschnitt).

Haftung bei Beschädigung/Verlust

Wird das private Gerät, das ein Arbeitnehmer (erlaubterweise) zur Arbeitsleistung einsetzt, gestohlen oder beschädigt, so stellt sich die Frage, wer die Kosten der Reparatur bzw. Wiederbeschaffung zu tragen hat.

Hier kann die Regelung beigezogen werden, die zur Verwendung privater Fahrzeuge für Dienstfahrten entwickelt wurde. Dienstfahrten fallen in das Betriebsrisiko des Arbeitgebers. Bei Beschädigung (oder Diebstahl) des Privatfahrzeugs während einer Dienstfahrt trägt grundsätzlich der Arbeitgeber die Reparatur- bzw. Wiederbeschaffungskosten[12]. Dies kann analog für private Geräte gelten, die zur Arbeitsleistung eingesetzt werden und während eines solchen geschäftlichen Einsatzes beschädigt (oder entwendet) werden.

Der Arbeitnehmer haftet seinerseits für den Schaden, den er dem Arbeitgeber absichtlich oder fahrlässig zufügt (Art. 321e OR). Ist eine Beschädigung (bzw. der Verlust) auf ein Verschulden des Arbeitnehmers zurückzuführen, so hat er für die entsprechenden Kosten aufzukommen. Je nach konkretem Einzelfall und Verschulden des Arbeitnehmers haftet er allenfalls auch nur anteilsmässig[13].

Toleriert ein Arbeitgeber ohne explizite Regelung die Verwendung privater Geräte, läuft er Gefahr, dass ein Arbeitnehmer einen Entschädigungsanspruch geltend macht.

Art. 321e OR ist einseitig zwingend (Art. 362 OR). Es kann nur zugunsten des Arbeitnehmers davon abgewichen werden, z.B. indem der Arbeitgeber die Reparaturkosten auch bei Fahrlässigkeit des Arbeitnehmers übernimmt. Art. 100 Abs. 1 OR beschränkt zudem den Bereich der zulässigen Regelung auf leichte und mittlere Fahrlässigkeit[14]. Von der Haftung des Arbeitnehmers bei Grobfahrlässigkeit und Absicht kann somit nicht abgewichen werden. Dem ist bei einer Regelung Rechnung zu tragen.

Kurz&bündig

«Bring Your Own Device» (BYOD) ist in vielen Unternehmen – ob bewusst oder nicht – wohl schon Realität. Arbeitgeber sollten sich deshalb mit den entsprechenden Fragestellungen auseinandersetzen, selbst wenn sie nicht beabsichtigen, eine BYOD-Strategie umzusetzen. Optiert ein Arbeitgeber für BYOD, so stellen sich arbeits- wie auch datenschutzrechtliche Fragen. Die Umsetzung der technischen Massnahmen muss auf die rechtlichen Vorgaben abgestimmt werden. Umgekehrt müssen die technischen Massnahmen auch mit organisatorischen Mitteln ergänzt und umgesetzt werden. Ein Arbeitgeber ist gut beraten, die relevanten Punkte in einer BYOD-Policy, entsprechenden Weisungen und Reglementen, allenfalls sogar im Arbeitsvertrag klar zu regeln. Mit einer möglichst klaren Regelung kann er spätere Probleme vermeiden und Haftungsrisiken minimieren.

Ausfallzeiten/Ersatzgeräte

Muss ein Gerät in die Reparatur bzw. wiederbeschafft werden, fragt sich, wer die entstehenden Ausfallzeiten zu tragen bzw. allenfalls für die Zeit der Reparatur ein Ersatzgerät zu stellen hat. Hier geht es wieder um die «Zurverfügungstellung der Arbeitsmittel» (Art. 327 OR). Bei Fehlen einer Regelung trägt der Arbeitgeber das Ausfallrisiko und hat damit dem Arbeitnehmer (vorübergehend) ein Ersatzgerät zur Verfügung zu stellen.

Betrieb, Support und Unterhalt

Der Betrieb des Gerätes eines Arbeitnehmers verursacht laufende Kosten. Solche können bei Laptops z.B. wiederkehrende Lizenzkosten für Software oder Verbindungskosten bei mobilem Einsatz, bei Smartphones z.B. Telefon- und Verbindungskosten sein. Auch Kosten für Support und Unterhalt können anfallen. Support kann etwa in der Unterstützung bei der Einrichtung, Bedienung oder Fehlerbehebung bestehen. Unterhalt umfasst namentlich den Ersatz defekter Teile.

Die «Entgrenzung» von Arbeits- und Privatsphäre kann zu Beeinträchtigungen der Gesundheit führen. So stellen sich Fragen zu den Ferien- und den zulässigen Arbeitszeiten.

Hier helfen die Regelungen zum Auslagenersatz im Allgemeinen (Art. 327a OR) sowie – analog angewandt – zum Auslagenersatz bei Benutzung eines privaten Fahrzeugs (Art. 327b OR) weiter. Gemäss Art. 327b Abs. 1 OR hat der Arbeitnehmer Anspruch auf Ersatz der üblichen Aufwendungen für laufende Kosten, Support und Unterhalt. Dies aber nur anteilsmässig, d.h. bei BYOD in dem Masse, wie das Gerät zu Arbeitszwecken eingesetzt wird.

Da die gesetzlichen Bestimmungen für Interpretationen offen sind, empfiehlt sich auch hier eine klare vertragliche Umschreibung. Dabei ist zu beachten, dass Art. 327a Abs. 1 und 327b Abs. 1 OR einseitig zwingend sind. Sie können somit nur zugunsten des Arbeitnehmers abgeändert werden (Art. 362 OR). Eine Regelung, wonach der Arbeitgeber die laufenden Kosten, Support und Unterhalt vollständig übernimmt, ist somit ohne Weiteres zulässig (und kann auch im Interesse des Arbeitgebers sein). Ebenfalls zulässig ist es, einen Anteil der Aufwendungen festzuhalten, welcher die geschäftliche Verwendung abdeckt, oder eine pauschale Abgeltung zu vereinbaren[15].

Eine weitere Frage stellt sich bezüglich der Amortisation, gerade bei IT-Geräten, die schnell veralten. Art. 327b Abs. 2 OR sieht für Fahrzeuge vor, dass der Arbeitgeber grundsätzlich Amortisationsbeiträge zu leisten hat. Im Gegensatz zu Art. 327b Abs. 1 OR kann von dieser Regelung aber abgewichen werden.

Ferien-/Arbeitszeiten

Art. 328 OR sieht eine allgemeine Fürsorgepflicht des Arbeitgebers vor, wozu insbesondere der Gesundheitsschutz zählt. Im Anwendungsbereich des ArG werden diese Pflichten in Art. 6 ArG sowie in der ArGV-3 konkretisiert[16]. Der Arbeitgeber hat aktiv Massnahmen zum Schutz der Arbeitnehmer zu treffen (Art. 328 Abs. 2 OR, Art. 6 Abs. 1–2 ArG)[17]. Die Arbeitnehmer sind entsprechend zu informieren und anzuleiten (Art. 5 ArGV-3).

Nutzt der Arbeitnehmer private Geräte (auch) für geschäftliche Zwecke, findet eine Vermischung von Privat- und Geschäftsbereich nicht nur in technischer, sondern auch in organisatorischer und zeitlicher Hinsicht statt. Einer der Beweggründe des Arbeitgebers, BYOD einzuführen, kann gerade in der erweiterten Verfügbarkeit des Arbeitnehmers liegen. Die Möglichkeit, das Gerät nach Feierabend, über das Wochenende oder während Ferien am Arbeitsort zu lassen bzw. auszuschalten, fällt zumeist weg. Private Geräte wollen ja auch ausserhalb des Geschäfts und der Geschäftszeiten genutzt werden. Diese «Entgrenzung» von Arbeits- und Privatsphäre kann zu Beeinträchtigungen der Gesundheit des Arbeitnehmers führen (Stress, Überlastung, Burnout, usw.)[18].

Es stellen sich somit Fragen zu den Ferienzeiten sowie (im Anwendungsbereich des ArG) zu den zulässigen Arbeitszeiten.

Der Ferienanspruch des Arbeitnehmers (Art. 329a OR) dient diesem zur Erholung und ist deshalb auch mit einem Abgeltungsverbot geschützt (Art. 329d Abs. 2 OR). Leistet der Arbeitnehmer während seiner Ferien trotzdem Arbeit (die privaten Geräte stehen ihm ja zur Verfügung), so verfehlen die Ferien ihren Erholungszweck. Der Arbeitgeber riskiert, dass er die Ferien erneut gewähren muss oder der Ferienanspruch per Ende des Arbeitsverhältnisses in einen Abgeltungsanspruch umgewandelt wird[19].

Bezüglich Arbeitszeiten gilt, dass sowohl Nacht- wie auch Sonntagsarbeit grundsätzlich verboten und nur im Ausnahmefall mit Bewilligung zulässig sind (Art. 10, 16 ff. ArG). Vorübergehende Nachtarbeit zwischen 23 und 6 Uhr ist mit einem Lohnzuschlag von mind. 25%

abzugelten (Art. 17b ArG), unabhängig davon, ob eine Bewilligung für Nachtarbeit eingeholt wurde oder nicht[20]. Dasselbe gilt für vorübergehende Sonntagsarbeit (zwischen Samstag 23 Uhr und Sonntag 23 Uhr), wobei hier der Lohnzuschlag sogar 50% beträgt (Art. 19 Abs. 3 ArG) und die geleistete Arbeitszeit durch Freizeit zu kompensieren ist (Art. 20 Abs. 2 ArG). Duldet der Arbeitgeber Arbeitsleistungen zu Nacht- oder Sonntagszeiten, bestehen für ihn die Risiken einer Lohnzuschlagsforderung sowie der Missachtung der Bewilligungspflicht (mit der allfälligen Konsequenz einer Geldstrafe, Art. 59 i.V.m. 61 ArG).

Sowohl unter dem Aspekt des Gesundheitsschutzes als auch demjenigen der Arbeits- und Ferienzeiten ist der Arbeitgeber somit gut beraten, eine klare Regelung auch des zeitlichen Einsatzes der privaten Geräte zu Geschäftszwecken vorzusehen.

Datenschutz

Übersicht

Aus der Warte des Datenschutzes[21] ist zuerst eine Unterscheidung nach den von BYOD betroffenen Daten zu machen. Auf der einen Seite sind Daten im Einflussbereich des Arbeitgebers betroffen (z.B. Daten von Kunden), auf der anderen Seite Daten des Arbeitnehmers selbst. Für beide ergeben sich bei BYOD Besonderheiten. Näher zu betrachten sind dabei insbesondere folgende Punkte:

- Datensicherheit,
- Haftungsfragen,
- Arbeitnehmerschutz.

Datensicherheit

Art. 7 DSG stellt Vorschriften zur Datensicherheit auf. Der Arbeitgeber muss die Sicherheit der durch ihn bzw. seine Arbeitnehmer bearbeiteten (Personen-)Daten durch ein ganzheitliches Sicherheitskonzept gewährleisten, welches bauliche, technische und organisatorische Massnahmen umfasst (vgl. Art. 8 ff. VDSG)[22]. Weitere Anforderungen an die Datensicherheit können sich zudem aus anderen gesetzlichen Verpflichtungen, aus Vertrag oder aus branchenspezifischen Vorschriften ergeben.

Je nach Ausgestaltung einer BYOD-Strategie werden Daten mit/auf Privatgeräten abgerufen, bearbeitet und allenfalls gespeichert. Die technischen Möglichkeiten reichen von zentraler Datenhaltung (mit Fernzugriff von Privatgeräten)[23] über Abruf und Bearbeitung von Daten in speziellen Anwendungen auf den Privatgeräten (sog. «Container-Apps»)[24] bis hin zur vollständigen Vermischung privater und geschäftlicher Daten.

Der technische[25] Aspekt der Datensicherheit lässt sich z.B. mittels MDM (Mobile Device Management) angehen, d.h. zentral verwalteter technischer Vorgaben und Einschränkungen für die betroffenen (Privat-)Geräte[26]. Die Umsetzung von MDM setzt Zugriff auf das Privatgerät voraus, was nur mit entsprechender Zustimmung des Arbeitnehmers möglich ist[27]. Eine solche Zustimmung sollte hinsichtlich Zeitpunkt, Umfang, Zugriffsberechtigter und Zweck möglichst klar umschrieben sein und schriftlich erfolgen.

Auf organisatorischer[28] Seite sind zusätzlich Weisungen an die Arbeitnehmer notwendig und spezielle Verhaltenspflichten zu stipulieren. Dies kann in allgemeinen Benutzungsreglementen und Sicherheitsvorgaben oder auch in einer speziellen «BYOD-Policy» erfolgen. Die Verhaltenspflichten sollten z.B. vorsehen, dass Privatgeräte Dritten nicht zugänglich gemacht werden dürfen[29]. Weiter ist insbesondere zu regeln, wie im Falle der Beendigung des Arbeitsverhältnisses vorzugehen ist. Hat der Arbeitgeber MDM-Software installiert (vgl. oben), kann beispielsweise eine Fernlöschung der Geschäftsdaten erfolgen. Werden dadurch aber auch private Daten des Arbeitnehmers beeinträchtigt, kann eine Persönlichkeitsverletzung vorliegen. Der Arbeitgeber sollte deshalb auch hier vorgängig für eine klare Trennung von privaten und geschäftlichen Daten sorgen. Dies kann durch allgemeine Reglemente oder durch eine spezifische BYOD-Policy erfolgen.

Der Arbeitgeber muss die Sicherheit der durch seine Arbeitnehmer bearbeiteten Personendaten durch ein ganzheitliches Sicherheitskonzept gewährleisten.

Haftungsfragen

Mit BYOD wird der Zugriffsbereich auf die im Unternehmen bearbeiteten Daten erweitert. Dies erhöht das Risiko in vielerlei Hinsicht. Die Gefahr eines unautorisierten Abrufs mittels ungenügend gesicherten Privatgeräten wird erhöht. Bei einem Verlust des Privatgerätes sind auch die darauf gespeicherten Daten verloren, sofern weder ein Backup noch eine zentrale Datenhaltung besteht. Ist ein Privatgerät zudem ungenügend geschützt, kann im Extremfall gar die gesamte IT-Infrastruktur des Unternehmens kompromittiert werden (z.B. durch Trojaner/Malware)[30].

Die Haftungsfrage stellt sich gleich doppelt, nämlich im Aussen- wie im Innenverhältnis.

Gegen aussen kann Dritten ein ersatzpflichtiger Schaden entstehen (z.B. einem Kunden des Unternehmens). Hier haftet der Arbeitgeber je nach Konstellation für den Arbeitnehmer als Hilfsperson (Art. 101 OR) oder selbst als Geschäftsherr (Art. 55 OR), sofern keine Haftungseinschränkung besteht (Art. 101 Abs. 2 OR) bzw. er den Sorgfaltsnachweis (Art. 55 Abs. 1 OR) nicht erbringen kann. Letzteres wird ihm indes nur möglich sein, wenn er seine Bemühungen zur Sicherstellung der IT-Sicherheit auch dokumentieren kann. Fehlen hier verbindliche Vorgaben an die Arbeitnehmer, wird ein Sorgfaltsnachweis schwierig.

Der Arbeitgeber ist verpflichtet, bei der Implementierung von Datensicherheitssystemen dem Schutz der Persönlichkeit des Arbeitnehmers Rechnung zu tragen.

Im Innenverhältnis, d.h. zwischen Arbeitgeber und Arbeitnehmer, können sich sowohl direkte Schäden (wie z.B. Wiederherstellungskosten bei Datenverlust) wie auch indirekte Schäden ergeben (z.B. durch Forderungen Dritter). Eine Haftung des Arbeitgebers gegenüber

Fussnoten

1 Das zu Beginn des BYOD-Trends oft vorgebrachte Argument der erhofften Kosteneinsparung hat sich inzwischen wohl als unzutreffend erwiesen.
2 Auf die betriebswirtschaftlichen und technischen Aspekte gehen wir hier nicht ein.
3 Bei CYOD (Choose Your Own Device) werden die Geräte zwar weiterhin vom Arbeitgeber gestellt, doch wird dem Arbeitnehmer eine Auswahl an zeitgemässen Geräten geboten, aus der er auswählen kann; bei PUOCE (Private Use of Company Equipment) wird den Arbeitnehmern die private Verwendung der Geschäftsgeräte erlaubt.
4 Wakefield Research, Global Survey: Dispelling Six Myths of Consumerization of IT.
5 Obligationenrecht (OR), SR 220.
6 Arbeitsgesetz (ArG), SR 822.11.
7 Insb. ArGV-1 (SR 822.111) und ArGV-3 (SR 822.113).
8 OR 327 geht damit bezüglich Auslagen für Arbeitsmittel als lex specialis dem allgemeinen Auslagenersatz gem. OR 327a vor, vgl. BSK OR I (2011) – Portmann, Art. 327 N 4.
9 Beranek Zanon, N 19; BSK OR I (2011) – Portmann, Art. 327 N 3.
10 Zu den Schranken des Weisungsrechts: Geiser, Die Änderungskündigung im schweizerischen Arbeitsrecht (in: AJP 1999, 60 ff.), N 1.2 ff., 60 f.; Geiser, Rechtsprobleme im Zusammenhang mit der Flexibilisierung der Arbeit (in: AJP 1998, 1019 ff.), 1022 f. N 3.9.
11 Zur Änderungskündigung grundlegend: BGE 123 III 246; zur Problematik betrieblicher Strukturveränderungen: Stöckli, Das Kündigungsrecht als Hindernis für betriebliche Strukturveränderungen (in: ArbR 2007, S. 191), 199 sowie Geiser, op.cit.
12 BSK OR I (2011) – Portmann, Art. 327b N 3.
13 Vgl. zur Schadenersatzbemessung und den Reduktionsgründen BSK OR I (2011) – Portmann, Art. 321e N 5 ff.
14 BSK OR I (2011) – Wiegand, Art. 100 N 4.
15 Wobei pauschale Abgeltungen aber mindestens die durchschnittlichen Betriebs- und Unterhaltskosten decken müssen, vgl. BSK OR I (2011) – Portmann, Art. 327b N 7.
16 Wobei die Vorschriften betr. Gesundheitsschutz (insb. ArG 6 und ArGV-3) auch auf Arbeitnehmer mit einer «höheren leitenden Tätigkeit» anwendbar sind (ArG 3a lit. b).
17 Diese Pflicht wird weiter ausgeführt in ArGV-3 sowie der Wegleitung des SECO zu den Verordnungen 3 und 4 zum Arbeitsgesetz (8. Überarbeitung, 2011), vgl. insb. S. 302-1 ff. Vgl. auch Letsch Thomas, Rechtliche Aspekte von Work-Life-Balance, Bern (2008), N 112 f., N 123 ff. und N 133 ff.
18 Letsch, op. cit., N 33 ff., insb. N 51 ff.
19 BGE 131 III 454, E. 2.2 (S. 454 f.); BSK OR I (2011) – Portmann, Art. 329d N 11.
20 OFK-Müller (2009), Kommentar ArG 17b Abs. 1; Stöckli/Soltermann, Stämpflis Handkommentar (2005), ArG 17b N 1.
21 Vgl. dazu das Datenschutzgesetz (DSG), SR 235.1 sowie die Verordnung zum DSG (VDSG), SR 235.11.
22 BSK DSG (2006)-Pauli, Art. 7 N 6.
23 Wie z.B. mit Citrix-Applikationen.
24 Vgl. zur sog. «Containerization»/«Containment»: Mitchell Robert, Best BYOD Management: Containment is your friend, in: Computerworld (29.8.2012), online: www.computerworld.com/s/article/9230476 (29.10.2012).
25 Vgl. dazu Rosenthal, Handkommentar DSG (2008), Art. 7 N 8.
26 Vgl. zu MDM z.B. Schlede Frank-Michael/Bär Thomas, Ratgeber: Mobile Device Management – den mobilen Geräte-Zoo im Griff behalten, in: Tecchannel (4.5.2012), online: <http://www.tecchannel.de/netzwerk/management/2039192> (29.10.2012).
27 Beranek Zanon, N 21 ff.
28 Vgl. dazu Rosenthal, Handkommentar DSG (2008), Art. 7 N 9.
29 Ein Laptop, auf dem Geschäftsdaten gespeichert bzw. ohne Passwortschutz zugänglich sind, dürfte dann beispielsweise nicht von der Tochter des Arbeitnehmers genutzt werden, um damit eine Arbeit für die Schule zu schreiben.
30 Vgl. auch Beranek Zanon, N 44 ff.
31 Vgl. dazu Wolfer Simon, Die elektronische Überwachung des Arbeitnehmers im privatrechtlichen Arbeitsverhältnis, Zürich (2008), N 474 ff.
32 Vgl. auch Seco, Wegleitung zur Verordnung 3 zum Arbeitsgesetz, ArGV 3 Art. 26: Überwachung der Arbeitnehmer (Stand: 1.2.2012).
33 Vgl. z.B. EDÖB, Leitfaden über Internet- und E-Mail-Überwachung am Arbeitsplatz (Juli 2009, Stand 22.1.2012).

dem Arbeitnehmer dürfte sich in erster Linie unter Art. 328 ff. OR ergeben, eine solche des Arbeitnehmers gegenüber dem Arbeitgeber unter Art. 321e OR (vgl. dazu Abschnitt «Haftung bei Beschädigung/Verlust»). Werden die Pflichten des Arbeitnehmers in entsprechenden Reglementen und Weisungen klar formuliert, kann eine Haftung des Arbeitnehmers eher bejaht werden, als wenn der Arbeitgeber die Verwendung von Privatgeräten zu geschäftlichen Zwecken ohne Vorgaben oder Regelungen duldet.

Arbeitnehmerschutz

Die Pflicht des Arbeitgebers zum Schutz der Persönlichkeit des Arbeitnehmers (Art. 328 OR) umfasst auch datenschutzrechtliche Belange (Art. 328b OR, DSG, ArGV-3).

Bei BYOD muss notwendigerweise ein bestimmter Grad von Kontrolle und Überwachung implementiert werden, um den Vorgaben zur Datensicherheit zu genügen (vgl. oben). Der Arbeitgeber ist verpflichtet, bei der Implementierung solcher Systeme dem Schutz der Persönlichkeit des Arbeitnehmers Rechnung zu tragen[31]. Weder dürfen private Daten des Arbeitnehmers davon betroffen sein (Schutz der Privatsphäre, Art. 328b OR), noch dürfen solche Massnahmen zu einer Überwachung des Arbeitnehmers selbst führen (Art. 26 ArGV-3)[32].

Um dies korrekt umzusetzen, sind die technischen Massnahmen auf die rechtlichen Vorgaben abzustimmen und die Arbeitnehmer sind entsprechend zu informieren[33]. Das kann je nach konkreter Situation in einem umfassenderen Reglement zur IT-/Internet-Nutzung generell erfolgen oder in einer spezifischen BYOD-Policy.

Zusammenfassung

Arbeitsrechtliche Vorgaben

Die arbeitsrechtlichen Vorgaben sind weitgehend dispositiv. Eine Regelung im Rahmen einer BYOD-Policy ist deshalb möglich und ratsam: Damit sich der Arbeitgeber nicht unverhofft in einer ungewollten Situation findet, sollte er die relevanten Punkte ausdrücklich (und schriftlich) regeln. Einzelne Punkte bedürfen allenfalls der Aufnahme in den Arbeitsvertrag. Ein Grossteil kann über entsprechende Weisungen und Reglemente geregelt werden.

Datenschutzrechtliche Vorgaben

Aus dem Datenschutzrecht ergeben sich verschiedene Pflichten technischer wie auch organisatorischer Natur. Einerseits ist diesen bei der Umsetzung einer BYOD-Strategie grundsätzlich Rechnung zu tragen. Andererseits sind die technischen Massnahmen mit entsprechenden Vorgaben in Reglementen und/oder Weisungen zu ergänzen. Dadurch kann ein Arbeitgeber, der eine BYOD-Strategie umsetzt, sowohl die Einhaltung datenschutzrechtlicher Pflichten sicherstellen als auch sein Haftungsrisiko minimieren. ■

Die arbeitsrechtlichen Vorgaben sind weitgehend dispositiv. Eine Regelung im Rahmen einer BYOD-Policy ist deshalb möglich und ratsam.

Literatur

- Beranek Zanon Nicole, Bring your own device (BYOD) aus rechtlicher Sicht, in: Jusletter IT (12.9.2012).
- Bradley Joseph, Loucks Jeff, Macaulay James, Medcalf Richard, Buckalew Lauren, Cisco Studienreport, BYOD: Ein Trend von globaler Tragweite, Cisco IBSG, 2012.
- Diverse, Bring Your Own Device (BYOD) – Topic Center, in: Computerworld online: <http://www.computerworld.com/s/topic/227/Bring+Your+Own+Device+(BYOD)> (29.10.2012).
- Heinzelmann Regula, Richtlinien für das Internet am Arbeitsplatz, 2007.
- Heinzelmann Regula, Über den Umgang mit Privatgeräten im Beruf, in: KMU-Magazin Nr. 10, Nov-2012.
- Müller Thomas, Herausforderung sicheres mobiles Arbeiten, in: IT-Security 2/12, 11 ff.
- Portmann Roland, Private Smartphones im Geschäftsumfeld, in: digma 2012, 42 ff.
- Tschol Daniela, «Bring your own» im Arbeitsalltag, in: IT business 1/2012, 2 f.
- von Kaenel Adrian, Die ständige Erreichbarkeit des Arbeitnehmers, in: ARV 2009, 1 ff.
- Wakefield Research, Global Survey: Dispelling Six Myths of Consumerization of IT, Januar 2012.