

# Arbeitsrecht Droit du travail

Zeitschrift für Arbeitsrecht und Arbeitslosenversicherung  
Revue de droit du travail et d'assurance-chômage

**Herausgegeben von / Publié par**

Prof. Dr. Wolfgang Portmann (Vorsitz/Présidence),  
Prof. Dr. Gabriel Aubert, Prof. Dr. Jean-Philippe Dunand,  
Dr. Adrian von Kaenel, Prof. Dr. Roland A. Müller,  
Dr. Boris Zürcher (SECO)

**ARV  
DTA**

**In Zusammenarbeit mit / En collaboration avec**

SECO (Staatssekretariat für Wirtschaft /  
Secrétariat d'Etat à l'économie)

3/2016

**Das Thema/Doctrine**

Bring Your Own Device (BYOD)

**Gesetzgebung/Législation**

**Rechtsprechung/Jurisprudence**

Urteilsbesprechungen/Commentaires d'arrêts

Urteilsauszüge/Extraits d'arrêts

**Literatur/Bibliographie**

Buchbesprechungen/Recensions

Hinweise auf Bücher und Beiträge/Livres et articles

**Mitteilungen/Nouvelles**

Aus Europa/Europe

Aus der ILO/OIT

**Offizieller Teil des SECO/Partie officielle du SECO**

## Impressum

**Zeitschrift für Arbeitsrecht und Arbeitslosenversicherung/Revue de droit du travail et d'assurance-chômage**  
ISSN 1660-0339, [www.arv-online.ch](http://www.arv-online.ch)

### Herausgeber / Editeurs

Prof. Dr. iur. Wolfgang Portmann (Vorsitz/Présidence),  
Ordinarius für Privat- und Arbeitsrecht an der  
Universität Zürich

Prof. Dr. iur. Gabriel Aubert, Professeur ordinaire au  
Département de droit du travail et de la sécurité sociale à  
l'Université de Genève, juge suppléant au Tribunal fédéral

Prof. Dr. iur. Jean-Philippe Dunand, Professeur  
ordinaire de droit romain, d'histoire du droit et du droit  
du travail à l'Université de Neuchâtel

Dr. iur. Adrian von Kaenel, Rechtsanwalt in Wetzikon,  
Lehrbeauftragter an der Universität Zürich

Prof. Dr. iur. Roland A. Müller, Titularprofessor für Obliga-  
tionen-, Arbeits- und Sozialversicherungsrecht an der  
Universität Zürich, Rechtsanwalt und nebenamtlicher  
Richter am Arbeitsgericht Zürich, Direktor des Schweizeri-  
schen Arbeitgeberverbandes

Dr. Boris Zürcher, Leiter der Direktion für Arbeit im SECO

### Korrespondenzadressen /

#### Adresses de correspondance

Prof. Dr. iur. Wolfgang Portmann, Universität Zürich,  
Rechtswissenschaftliche Fakultät, Rämistrasse 74/16,  
8001 Zürich, Tel. 044 634 21 80  
[lst.portmann@rwi.uzh.ch](mailto:lst.portmann@rwi.uzh.ch)

Offizieller Teil des SECO: SECO – Staatssekretariat für  
Wirtschaft, Direktion für Arbeit, TCRV, Effingerstrasse 31,  
3003 Bern, Tel. 031 322 29 20, [tcrv@seco.admin.ch](mailto:tcrv@seco.admin.ch)

### Erscheinungsweise / Parution

4x jährlich

### Abonnementspreise / Prix de l'abonnement

Jahresabonnement: CHF 128.00

Jahresabonnement für Studierende: CHF 89.00

Einzelheft: CHF 35.00

### PrintPlus

Mit dem PrintPlus-Abonnement haben Sie die Möglich-  
keit, Ihre Zeitschrift digital zu lesen. Zeitgleich mit  
der Printausgabe haben Sie Zugang zu den Beiträgen in  
digitaler Form. Detaillierte Informationen finden  
Sie unter [www.schulthess.com/printplus](http://www.schulthess.com/printplus)

Jahresabonnement: CHF 144.00

Jahresabonnement für Studierende: CHF 99.00

### Inserate / Annonces

Zürichsee Werbe AG

Herr Pietro Stuck, Seestrasse 86, 8712 Stäfa  
[pietro.stuck@zs-werbeag.ch](mailto:pietro.stuck@zs-werbeag.ch), +41 (0)44 928 56 17

### Verlag und Abonnementsverwaltung /

#### Edition et administration

Schulthess Juristische Medien AG  
Zwingliplatz 2, Postfach, 8021 Zürich,  
Tel. +41 44 200 29 29, Fax +41 44 200 29 28  
[www.schulthess.com](http://www.schulthess.com), [zs.verlag@schulthess.com](mailto:zs.verlag@schulthess.com)

## Inhaltsübersicht / Sommaire

|                                                                               |            |
|-------------------------------------------------------------------------------|------------|
| <b>Das Thema / Doctrine .....</b>                                             | <b>151</b> |
| Bring Your Own Device (BYOD)<br>(Isabelle Wildhaber/Silvio Hänsenberger)..... | 151        |
| <b>Gesetzgebung / Législation .....</b>                                       | <b>166</b> |
| <b>Rechtsprechung / Jurisprudence .....</b>                                   | <b>181</b> |
| <i>Urteilsbesprechungen / Commentaires d'arrêts</i>                           |            |
| Arbeitsvermittlung (Michael Kull).....                                        | 181        |
| <i>Urteilsauszüge / Extraits d'arrêts.....</i>                                | <i>186</i> |
| <b>Literatur / Bibliographie .....</b>                                        | <b>208</b> |
| <i>Buchbesprechungen / Recensions.....</i>                                    | <i>208</i> |
| Albrecht, Kathrin:<br>Prämien im Berufsfussball .....                         | 208        |
| <i>Hinweise auf Bücher und Beiträge / Livres et articles</i>                  | <i>212</i> |
| <b>Mitteilungen / Nouvelles .....</b>                                         | <b>218</b> |
| Aus Europa / Europe .....                                                     | 218        |
| Aus der ILO / OIT .....                                                       | 221        |
| <b>Offizieller Teil des SECO /<br/>Partie officielle du SECO .....</b>        | <b>223</b> |

# Bring Your Own Device (BYOD)

## Wie man den Einsatz privater mobiler Geräte im beruflichen Umfeld gestaltet, damit er nicht zum «Bring Your Own Disaster» wird

Prof. Dr. Isabelle Wildhaber, LL.M.

Silvio Hänsenberger, M.A. HSG

*BYOD ist die geschäftliche Nutzung eines mobilen privaten Gerätes. Der Nutzeffekt von Privatgeräten am Arbeitsplatz ist unbestritten. Gleichzeitig gilt es, die Sicherheit und Informationsgüter sowie die Privatsphäre der Arbeitnehmer zu gewährleisten. Dazu werden immer öfter entsprechende Nutzungsrichtlinien festgelegt. Ist in gewissen Branchen die Datensicherheit sehr wichtig, ist zu überlegen, ob nicht ein Choose Your Own Device (CYOD) eine bessere Lösung ist. BYOD wirft viele rechtliche Risiken auf, die in diesem Beitrag analysiert werden. Diese reichen von der Freiwilligkeit über die Kostentragung und die Haftung bis hin zu datenschutzrechtlichen Problemen.*

*BYOD est l'utilisation professionnelle d'appareils privés. Leur utilité au travail est incontestée. Il convient cependant d'assurer la sécurité, ainsi que la protection des informations et de la sphère privée du salarié. De plus en plus souvent sont établies, à cette fin, des directives d'utilisation. Dans certaines branches où la sécurité des données est particulièrement importante, il faut se demander si une solution préférable ne serait pas Choose Your Own Device (CYOD). BYOD entraîne beaucoup de risques juridiques, ici analysés, qui vont de la notion de volontariat à celles de couverture des frais, de responsabilité et de protection des données.*

### Inhaltsübersicht

- I. Einleitung
- II. Chancen und Risiken von BYOD
- III. Rechtliche Problemfelder
  - 1. Freiwilligkeit von BYOD
  - 2. Kostentragung bei BYOD

- 3. Haftpflichtrechtliche Fragen bei BYOD
  - a) Haftung des Arbeitgebers
  - b) Haftung des Arbeitnehmers
- 4. Datenschutzrechtliches Minenfeld
- 5. Regelungskompetenz des Arbeitgebers
- 6. Arbeitsgesetz und BYOD
- IV. BYOD-Richtlinien
- V. Schlusswort

### I. Einleitung

«Bring Your Own Device» heisst «Bringen Sie Ihr Eigenes Gerät». Es bedeutet, dass ein mobiles Gerät (meist Smartphone, Laptop oder Tablet), welches vom Arbeitnehmer mit eigenen Mitteln zu privaten Zwecken erworben worden ist, auch geschäftlich ge-

nutzt wird<sup>1</sup>. BYOD erfolgt oft unter Einbindung in das IT-System und die Infrastruktur des Arbeitgebers. Es geht aber bei BYOD um mehr als die Nutzung der Geräte. Arbeitnehmer kaufen, administrieren und organisieren die Hardware und die Software selbständig; sie sind Eigentümer des Gerätes.

<sup>1</sup> S. dazu ausführlich Sébastien Fanti, Bref aperçu des aspects légaux du BYOD (Bring Your Own Device), in: Jean-Philippe Dunand/Pascal Mahon (Hrsg.), Internet au travail, Genf 2014, S. 165 ff.; ebenso Roland Mathys, Regelungsbedarf bei Bring Your Own Device, Schellenberg Wittmer Newsletter April 2015, S. 1, <<http://www.swlegal.ch>>.

BYOD liegt im Trend. Eine aktuelle internationale Statistik zeigt, dass heute 59% der Unternehmen BYOD ermöglichen, und weitere 13% der Unternehmen den Einsatz von BYOD in absehbarer Zeit planen<sup>2</sup>. In einer anderen Umfrage nennen 61% der Teilnehmer die verbesserte Mitarbeiter-Mobilität, 56% eine grössere Mitarbeiter-Zufriedenheit, 55% höhere Produktivität und 47% reduzierte Kosten als wichtigste Gründe für die Einführung von BYOD<sup>3</sup>. Als grösste Hemmschwellen für den Einsatz von BYOD nennen 39% der befragten Unternehmen Sicherheitsbedenken sowie 12% der Umfrageteilnehmer Bedenken wegen des Schutzes der Privatsphäre der Mitarbeiter<sup>4</sup>.

BYOD kann viele rechtliche Risiken verursachen und wirft grundsätzliche Fragen der «Waffengleichheit» zwischen Arbeitgeber und Arbeitnehmer auf, die im Folgenden analysiert werden sollen. Zu diesem Zweck werden zunächst die Chancen und Risiken sowie das mögliche, in unseren Augen grosse Konfliktpotential von BYOD betrachtet (nachfolgend II.). Anschliessend wendet sich der Beitrag rechtlichen Fragestellungen zu: Haben die Arbeitnehmer eine Pflicht zu BYOD oder ein Recht dazu (nachfolgend III.1.)? Wer trägt welche Kosten (nachfolgend III.2.)? Wer haftet für welche Risiken (nachfolgend III.3.)? Welches sind die datenschutzrechtlichen Stolpersteine, welche mit BYOD einhergehen (nachfolgend III.4.)? Was ist die Regelungskompetenz des Arbeitgebers, um die Nutzung privater Geräte des Arbeitnehmers festzulegen (nachfolgend III.5.)? Wie verträgt sich BYOD mit den arbeitsgesetzlichen Vorgaben (nachfolgend III.6.)? Nicht behandelt werden Fragen des geistigen Eigentums (Intellectual Property, IP), lizenzrechtliche und strafrechtliche Problemstellungen<sup>5</sup>. Rechtliche Problemfelder im Zusammenhang mit BYOD resultieren häufig aus fehlenden oder unklaren Regelungen, missbräuchlicher Nutzung und unzulässiger Überwachung. Der vorliegende Beitrag hat deshalb zum Ziel, mögliche rechtliche Probleme zu klären und Lösungsmöglichkeiten zu skizzieren,

insbesondere indem mögliche Klauseln für sog. BYOD-Richtlinien (nachfolgend IV.) vorgeschlagen werden. Wenn man sich denn für BYOD entscheidet, so kann durch solche BYOD-Guidelines vermieden werden, dass der Einsatz privater Endgeräte im geschäftlichen Umfeld zum «Bring Your Own Disaster» wird<sup>6</sup>. So nämlich wird BYOD oft scherzhaft übersetzt, unseres Erachtens nicht zu Unrecht.

## II. Chancen und Risiken von BYOD

BYOD bringt viele Chancen. Arbeitgeber, welche ihren Arbeitnehmern die Nutzung privater Geräte zur Erbringung der Arbeitsleistung ermöglichen, erhoffen sich u.a. Produktivitätsgewinne und Kosteneinsparungen<sup>7</sup>. Die Nutzer verwalten und administrieren ihre Geräte selbst. Mit privaten Geräten arbeiten Menschen oft schneller und kundiger als mit einem Geschäftsgerät. Des Weiteren kann BYOD *state-of-the-art*-Technologien und die Mitarbeiterzufriedenheit fördern. Oft wird als Chance für BYOD angeführt, dass die Arbeitnehmer von überall aus arbeiten könnten. Sie besäßen so Souveränität über ihre Arbeitszeiten und könnten Arbeiten dezentralisiert und flexibel organisieren und durchführen. Kommunikations- und Prozesswege im Unternehmen würden verkürzt. Unternehmen positionierten sich als moderne, attraktive Arbeitgeber am Arbeitsmarkt. Allerdings können diese Chancen auch durch mobile Geräte des Arbeitgebers wahrgenommen werden. Auch Geschäfts-Laptops und Geschäfts-Smartphones fördern die dezentrale und flexible Arbeit. Daneben gewinnt BYOD im Rahmen der Industrie 4.0 und der Optimierung von Betriebsabläufen zusätzlich an Bedeutung<sup>8</sup>.

<sup>2</sup> Teena Maddox, BYOD, IoT and wearables thriving in the enterprise, Tech Pro Research 4.1.2016, <<http://www.techproresearch.com/article/byod-iot-and-wearables-thriving-in-the-enterprise/>>.

<sup>3</sup> Crowd Research Partners, BYOD & Mobile Security, S. 6, <[http://www.crowdresearchpartners.com/portfolio\\_item/byod-mobile-security-report/](http://www.crowdresearchpartners.com/portfolio_item/byod-mobile-security-report/)>.

<sup>4</sup> Crowd Research Partners (Fn. 3), S. 9.

<sup>5</sup> S. dazu Fanti (Fn. 1), S. 194 ff. zum Strafrecht, S. 198 ff. zum IP und Lizenzrecht.

<sup>6</sup> Oliver Zöll/Jacek B. Kielkowski, Arbeitsrechtliche Umsetzung von «Bring Your Own Device» (BYOD), BB 2012, S. 2625 ff., S. 2625.

<sup>7</sup> Zu Chancen und Risiken von BYOD: Fraunhofer IAIS, Bring your own Device at my Company, <[https://www.iais.fraunhofer.de/fileadmin/user\\_upload/Abteilungen/ART/pdfs/IAIS\\_ART\\_BYOD\\_Poster\\_BringYourOwnDevice\\_v1.0.3.pdf](https://www.iais.fraunhofer.de/fileadmin/user_upload/Abteilungen/ART/pdfs/IAIS_ART_BYOD_Poster_BringYourOwnDevice_v1.0.3.pdf)>; Dean Wiech, The Benefits And Risks Of BYOD, Manufacturing Business Technology 28.1.2013, <<http://www.mbtmag.com/article/2013/01/benefits-and-risks-byod>>; Jen A. Miller, BYOD – the tech revolution that wasn't, CIO 20.8.2015, <<http://www.cio.com/article/2973977/byod/byod-the-tech-revolution-that-wasn-t.html>>.

<sup>8</sup> S. zu Integration von BYOD in Industrie 4.0: Hans Markus Wulf/Clemens Burgenmeister, Industrie 4.0 in der Logistik – Rechtliche Hürden beim Einsatz neuer Vernetzungs-Technologien, Computer und Recht 6/2015, S. 404 ff., 411 f.

Demgegenüber bestehen bei der geschäftlichen Nutzung privater Geräte auch *Risiken*<sup>9</sup>. Wie das KMU-Portal des Staatssekretariats für Wirtschaft (SECO) warnt, werden Smartphones und Tablets von vielen Schweizer Firmen als voll funktionsfähige tragbare Arbeitsplätze eingeführt, ohne Risikobewertung in Bezug auf Sicherheit und Gesundheit<sup>10</sup>. Sofern keine ausreichenden technischen Sicherheitsmassnahmen ergriffen werden oder falls notwendige Sicherheitsvorgaben durch den Arbeitgeber oder Arbeitnehmer ignoriert werden, besteht die Gefahr, dass Dritte auf Daten des Gerätes zugreifen können. Eine mögliche Sicherheitsmassnahme kann die Trennung von privater und geschäftlicher Softwareumgebung auf dem BYOD-Gerät sein. Dabei ist das Gerät entweder bereits vom Hersteller auf eine solche Unterscheidung ausgelegt (teilweise Smartphones der Marke «Blackberry») oder es wird nachträglich eine Software aufgespielt, mit der für die geschäftliche Nutzung ein gesonderter Bereich des Speichers abgegrenzt wird (Container)<sup>11</sup>. Die Daten in diesem Container werden verschlüsselt, und es gelten darin spezielle Regeln, nämlich die des Arbeitgebers. Verbinden sich BYOD-Geräte ausserhalb der Arbeitsumgebung mit dem Netzwerk oder Servern des Arbeitgebers, kann der Datenstrom mittels verschlüsselter Verbindung (z.B. durch ein virtuelles privates Netzwerk, VPN) abgesichert werden. Diese Verbindung kann dann auch für geschäftliche Telefonanrufe mittels Internet-Telefonie (Voice over IP, VoIP) genutzt werden.

Wenn Arbeitnehmer mit dem BYOD-Gerät öffentlich zugängliche Netzwerke ohne Verschlüsselung geschäftlich nutzen oder Daten auf Geräte oder Server überspielen, welche nicht genügend gegen Zugriffe Dritter (z.B. unverschlüsselte Backups in einem Cloud-Speicher), Schadsoftware, Verlust oder Diebstahl gesichert sind, besteht eine akute Gefährdung der betreffenden Daten. Unseres Erachtens sind deshalb sowohl aus Arbeitgeber- wie auch aus Arbeitnehmer-sicht Bedenken gegen BYOD aus datenschutzrechtlicher Sicht berechtigt. Für den Arbeitgeber, aber auch für den Arbeitnehmer besteht ein Sicherheitsrisiko. Der Verlust eines Smartphones, aber auch die Beendigung des Arbeitsverhältnisses oder eine Freistel-

lung, können für den Arbeitgeber aufgrund der vertraulichen Daten mit einem sehr hohen IT-Sicherheitsrisiko verbunden sein. Die Nutzung von unsicherer oder illegaler Software kann problematisch sein. Durch unvorsichtiges Installieren von Software kann schädliche Malware mitinstalliert werden, die auf die sensiblen Unternehmensdaten zugreift oder Unternehmensprozesse angreift. Ausserdem ist die Sicherheit der Daten durch allfällige Manipulationen wie «Jailbreaking» (nicht-autorisiertes Entfernen von Nutzungsbeschränkungen) gefährdet. Daraus kann sich die Notwendigkeit ergeben, den (auch privaten) Nutzungsumfang der Geräte zu beschränken, was wegen der Eigentümerstellung der Arbeitnehmer an den Geräten nicht unproblematisch ist<sup>12</sup>. BYOD kann auch zu IT-Supportproblemen führen, da die IT des Unternehmens verschiedene Geräte und Betriebssysteme unterstützen muss. Dies kann zu grossen Kosten führen (s. unten III.2.). Zudem hat BYOD auch einen psychologischen Einfluss auf die Arbeitnehmer: Für viele sind die mobilen Geräte ein Stressfaktor<sup>13</sup>. Sie lassen den Druck entstehen, stets flexibel und verfügbar zu sein und fördern die Sucht nach Information und die Angst, eine wichtige Information nicht rechtzeitig zu bemerken<sup>14</sup>. Ein weiteres Risiko von BYOD ist, dass gewisse Aufbewahrungspflichten teilweise nicht gewährleistet werden können, wenn ausserhalb des Arbeitsplatzes keine Backups erstellt werden<sup>15</sup>.

Mit BYOD gehen demnach sowohl Chancen wie auch Risiken einher. Wie Roland Mathys zu Recht schreibt, bringt BYOD ein *Konfliktpotential* mit sich, welches sich aus den diametral entgegenstehenden Bedürfnissen von Arbeitgeber und Arbeitnehmer ergibt<sup>16</sup>:

<sup>9</sup> S. dazu die Quellen in Fn. 7.

<sup>10</sup> <<http://www.kmu.admin.ch>>.

<sup>11</sup> Vgl. dazu Johannes Wendt, Bring your own device: Container auf dem Smartphone, Zeit Online 2.4.2013, <<http://www.zeit.de/digital/mobil/2013-03/computer-arbeitsplatz-byod-container>>.

<sup>12</sup> Das Verbot der Nutzung unsicherer Software dürfte keine unzumutbare Benachteiligung des Arbeitnehmers darstellen. Eine permanente Überwachungssoftware oder ein «wipe» (Löschung der gesamten Daten mittels eines installierten Dienstprogramms des Arbeitgebers) dürfte unangemessen sein. S. Zöll/Kielkowski (Fn. 6), S. 2627; Nicolas Birkhäuser/Marcel Hadorn, BYOD – Bring Your Own Device, Private Smartphones im geschäftlichen Arbeitsumfeld, SJZ 109/2013, S. 201 ff., S. 203 und S. 205 mit Verweis auf Art. 144<sup>bis</sup> StGB.

<sup>13</sup> Mark A. Reutter/Samuel Klaus, Rechtliche Stolpersteine bei «BYOD», digma 2012, S. 160 ff., S. 162; Thomas Letsch, Rechtliche Aspekte von Work-Life-Balance, Diss. Zürich, Bern 2008, N 33 ff., N 51 ff.; Fanti (Fn. 1), S. 173 ff.

<sup>14</sup> <<http://www.kmu.admin.ch>>; Fanti (Fn. 1), S. 173 ff.

<sup>15</sup> Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), Erläuterungen zu Bring your own Device, Bern 2014, <<http://www.edoeb.admin.ch/datenschutz/00739/01250/index.html?lang=de>>.

<sup>16</sup> So Mathys (Fn. 1), S. 1.

Der Arbeitgeber hat ein Interesse, die geschäftliche Nutzung von Geräten zu regeln, unabhängig davon, wem diese Geräte gehören. Die Arbeitnehmer erwarten, dass sie über ihre eigenen Geräte frei verfügen können. Daraus ergibt sich ein Konfliktpotential, gerade auch dann, wenn die geschäftliche Nutzung privater Geräte ohne BYOD-Policy und ohne Wissen des Arbeitgebers stattfindet. Der Arbeitgeber muss sich fragen, ob in seinem Betrieb die Chancen von BYOD die Risiken überwiegen. Eine IT-Strategie, die BYOD ermöglicht, steht zusammengefasst vor zwei Herausforderungen: Zum einen greifen auf das Unternehmensnetzwerk und die dort gespeicherten Daten sowohl unternehmenseigene als auch Privatgeräte zu und zum anderen werden die Geräte sowohl für berufliche als auch für private Zwecke genutzt.

### III. Rechtliche Problemfelder

#### 1. Freiwilligkeit von BYOD

Den Arbeitnehmer trifft *keine Pflicht zu BYOD*. Ein Arbeitnehmer kann mittels einer Weisung des Arbeitgebers grundsätzlich nicht zur Teilnahme an BYOD verpflichtet werden. Der Arbeitgeber hat die notwendigen Arbeitsgeräte zur Verfügung zu stellen (Art. 327 Abs. 1 OR)<sup>17</sup>. BYOD kann also nur freiwillig, mit Einwilligung des Arbeitnehmers, eingeführt werden. Arbeitnehmer können die Teilnahme an einem zwingenden BYOD-Programm verweigern oder sich daraus zurückziehen.

Ein BYOD kann entweder mit Beginn des Arbeitsverhältnisses oder während eines laufenden Arbeitsvertrags eingeführt werden. In beiden Konstellationen können sich grundsätzliche Fragen der «Waffengleichheit» stellen. Wenn der Arbeitgeber aus Kostengründen ein BYOD grossflächig einführen will, so kann es für die Arbeitnehmer faktisch schwierig sein, sich diesem zu verweigern. Da Änderungen des Arbeitsvertrages mittels einer *Änderungskündigung* durchgesetzt werden können<sup>18</sup>, kann der Arbeitneh-

mer vor der Wahl stehen, in Bälde seine Kündigung zu erhalten oder sein privates Gerät auch für berufliche Zwecke zu nutzen. Man kann sich deshalb die Frage stellen, ob eine solche Änderungskündigung nicht als missbräuchlich qualifiziert werden könnte. Dies ist von Fall zu Fall zu entscheiden. Relevant ist sicherlich, ob der Arbeitgeber die notwendigen Datenschutzmassnahmen trifft und damit die Datenschutzrechte des Arbeitnehmers garantieren kann. In BGE 118 II 157 hatte das Bundesgericht erwogen, eine Änderungskündigung als missbräuchlich anzusehen, wenn die Änderung als unbillig bezeichnet werden müsse. In BGE 123 III 246 wird klargestellt, dass eine Änderungskündigung zwar nicht in jedem Fall missbräuchlich im Sinne von Art. 336 OR sein müsse, dies aber sein könne. Ein BYOD gegen den Willen des Arbeitnehmers greift unzulässig in den privaten Bereich ein und steht ausserdem im Widerspruch zu Art. 327 Abs. 1 OR – sofern das Zurverfügungstellen privater Arbeitsgeräte nicht branchenüblich ist. Eine Kündigung, die vom Arbeitgeber ausgesprochen wird, weil sich der Arbeitnehmer nicht bereit erklärt, die Änderung der vertraglichen Arbeitsbedingungen zu akzeptieren, kann deshalb unseres Erachtens unter Umständen missbräuchlich sein. Es handelt sich um eine wesentliche Beeinträchtigung der Selbstbestimmung, wenn Privates und Geschäftliches in dieser Form gegen den Willen des Arbeitnehmers vermischt werden. Ein BYOD lässt sich in diesem Sinne «sachlich nicht rechtfertigen»<sup>19</sup>.

Arbeitgeber sollten auch inskünftig weiter über einen ausreichenden «Gerätepool» verfügen, um Arbeitnehmer die für die Aufgabenerfüllung notwendigen Arbeitsinstrumente zur Verfügung stellen zu können. Ansonsten setzt der Arbeitgeber sich der Gefahr eines möglichen Annahmeverzuges aus (Art. 324 Abs. 1 i.V.m. Art. 91 OR)<sup>20</sup>.

<sup>17</sup> Mathys (Fn. 1), S. 2; Isabelle Wildhaber/Silvio Hänsenberger, Internet am Arbeitsplatz, ZBJV 2016, S. 307 ff.; Christoph Holenstein, Die Benutzung von elektronischen Kommunikationsmitteln (Internet und Intranet) im Arbeitsverhältnis, Diss. Bern, Bern 2002, S. 53 f.

<sup>18</sup> Isabelle Wildhaber, Die Änderung von Arbeitsbedingungen bei Umstrukturierungen, Jusletter vom 21.4.2008.

<sup>19</sup> Vgl. Isabelle Wildhaber, Das Arbeitsrecht bei Umstrukturierungen, Habil., Zürich 2011, S. 266; BGE 123 III 250; Marco Kamber, Die Änderungskündigung im Arbeitsvertragsrecht. Insbesondere die Rechtsprechung zur Missbräuchlichkeit, Diss. Basel, Zürich 2014, Rz. 602 ff.

<sup>20</sup> Vgl. auch Fanti (Fn. 1), S. 171 f. (30-tägige Kündigungsfrist für den Arbeitnehmer und Schadenersatzpflicht des Arbeitnehmers).

Der Arbeitnehmer hat aufgrund des Weisungsrechts des Arbeitgebers (Art. 321d OR)<sup>21</sup> juristisch gesehen *kein Recht auf BYOD*<sup>22</sup>, auch wenn junge Arbeitnehmer teilweise von einem «Recht» ausgehen mögen, ihre eigenen Smartphones im Arbeitsumfeld zu nutzen<sup>23</sup>. Dennoch findet in der Realität eine solche Nutzung oft statt. Wenn der Arbeitgeber über die Nutzung privater Geräte für berufliche Zwecke Kenntnis hat und diese duldet, kann in gewissen Konstellationen von einem *stillschweigenden Einverständnis* ausgegangen werden. Weil damit aber Kosten- und Haftungsfolgen auf den Arbeitgeber zukommen können, ist eine BYOD-Richtlinie dringend zu empfehlen.

## 2. Kostentragung bei BYOD

Im Zusammenhang mit einem BYOD-Endgerät können *verschiedene Kosten* anfallen, bei denen sich die Frage stellt, ob sie vom Arbeitgeber oder vom Arbeitnehmer zu tragen sind.

Dabei kann es sich insbesondere um folgende Kosten handeln:

- *Anschaffungskosten*: Anschaffungskosten umfassen nicht nur die Kosten für das Gerät selbst, sondern auch Ausgaben für Software (z.B. Antiviren-/Textverarbeitungsprogramme), die geschäftlich genutzt wird.
- *Verbindungskosten/Roaming*
- *Abonnementskosten*
- *Amortisationskosten*
- *Stromkosten*: Dabei handelt es sich z.B. um die Kosten für das Aufladen eines Gerätes zuhause. Diese Kosten dürften zwar kaum ins Gewicht fallen, trotzdem erscheint eine Berücksichtigung für eine umfassende Regelung sinnvoll.
- *Lizenzkosten* (z.B. für Antiviren-, Textverarbeitungsprogramme): Lizenzbedingungen privater Software erlauben unter Umständen keine geschäftliche Nutzung. Für den Erwerb einer geschäftlichen Lizenz können zusätzliche Kosten entstehen.

- *Supportkosten*: Kosten für die Unterstützung bei technischen Problemen mit BYOD-Geräten (s. dazu auch oben II.).
- *Reparaturkosten und Kosten eines Ersatzgerätes* (Abgeltung des Schaden-<sup>24</sup>, Diebstahl- und Verlustrisikos). Diese Risiken können z.B. mit einer Beteiligung an einer entsprechenden Versicherungsprämie (z.B. Versicherung für Mobilgeräte) abgegolten werden. Aus Arbeitgebersicht ist darauf Wert zu legen, dass die getroffene Versicherungslösung auch die geschäftliche Nutzung des BYOD-Gerätes abdeckt. Ansonsten kann er für diese Schäden nach wie vor haftbar sein (s. unten III.3.a.).

Bei der Frage, wer welche Kosten zu tragen hat, ist zwischen den verschiedenen Kosten zu unterscheiden.

Die *Anschaffungskosten* werden beim BYOD mindestens teilweise von den Arbeitnehmern übernommen; ansonsten liegt kein BYOD vor. Der Arbeitgeber kann sich entweder unmittelbar an diesen Kosten beteiligen oder er bezahlt während der Dauer der BYOD-Nutzung einen anteilmässigen Betrag im Rahmen eines periodischen Amortisationsbeitrags. Bei BYOD handelt es sich per Definition um ein privates Gerät, das im Eigentum des Arbeitnehmers steht. Allfällige Vergünstigungen aufgrund von *Fringe Benefits* haben keinen Einfluss auf die sachenrechtliche Behandlung.

Grundsätzlich gilt gemäss Art. 327a OR, dass der Arbeitgeber arbeitsbegründete notwendige Arbeitnehmersauslagen zu ersetzen hat. Dieser Anspruch auf Auslagenersatz betrifft die variablen Gebühren für Mobilfunk und Datenverbindungen. Wenn diese Gebühren geschäftlich begründet sind, so hat der Arbeitgeber die *Verbindungskosten* (Mobilfunk-/Datenverbindungs-Gebühren) als Auslagenersatz zu übernehmen<sup>25</sup>.

Bei *Abonnements- und Amortisationskosten* dürfte hingegen eine Kostenbeteiligung angemessen sein, welche sich nach dem Anteil der geschäftlich be-

<sup>21</sup> Jean-Philippe Dunand, Internet au travail: droits et obligations de l'employeur et du travailleur, in: Jean-Philippe Dunand/Pascal Mahon (Hrsg.), Internet au travail, Genf 2014, S. 33 ff., S. 34; Holenstein (Fn. 17), S. 50.

<sup>22</sup> Reutter/Klaus (Fn. 13), S. 161; Fanti (Fn. 1), S. 170.

<sup>23</sup> Ellen Messmer, Young employees say BYOD a «right» not «privilege», Network World, 19.6.2012, <<http://www.infoworld.com/article/2617262/byod/young-employees-say-byod-a-right-not-privilege-.html>>.

<sup>24</sup> Analog zur Möglichkeit des Arbeitgebers, das Unfallrisiko bei der Amortisation eines durch den Arbeitnehmer zur Verfügung gestellten Motorfahrzeuges einzurechnen, vgl. dazu Ullin Streiff/Adrian von Kaenel/Roger Rudolph, Arbeitsvertrag, Praxiskommentar zu Art. 319–362 OR, 7. Aufl., Zürich 2012, Art. 327b N 2, 4.

<sup>25</sup> Manfred Rehbindler/Jean-Fritz Stöckli, Berner Kommentar, Bern 2010, Art. 327a N 3; Streiff/von Kaenel/Rudolph (Fn. 24), Art. 327a N 2.

gründeten Verwendung an der Gesamtnutzung richtet<sup>26</sup>. Anders wäre die Lage bei Abonnementskosten zu beurteilen, welche erst wegen der geschäftlichen Nutzung anfallen, wie z.B. der Abschluss einer Zusatzoption oder einer Flatrate für eine Geschäftsreise ins Ausland<sup>27</sup>. Diese Abonnementskosten müsste der Arbeitgeber übernehmen.

Allerdings kann die *Festlegung der Kostenteilung im Einzelfall schwierig* sein. Zunächst würde eine manuelle Erhebung der Nutzungsart durch den Arbeitnehmer die Produktivitätsgewinne durch BYOD vernichten. Deshalb kommen nur technische Massnahmen in Frage. Der geschäftliche Nutzungsumfang kann mit entsprechender Software erhoben werden. Problematisch erscheinen Aufzeichnungen über die private Nutzung, um mit ihnen den Anteil an der Gesamtnutzung zu erheben. Dazu muss auf private Daten des Arbeitnehmers zugegriffen werden. Letzteres bedarf aber zwingend der konkreten Zustimmung des Arbeitnehmers (s. unten III.4.). Neben dem Eingriff in die Persönlichkeitsrechte des Arbeitnehmers erscheint eine technische Lösung auch aus einem weiteren Grund als problematisch. Wird Software des Arbeitgebers auf dem Gerät des Arbeitnehmers installiert, handelt es sich dabei um ein Arbeitsmittel im Sinne von Art. 327 OR. Der Arbeitgeber hat diesbezüglich den notwendigen IT-Support zur Verfügung zu stellen. Im Zweifel wird dieser auch bei Fehlern im privat genutzten Teil des Gerätes beigezogen, was zu finanziellem Aufwand führen kann, der die Kosteneinsparungen durch BYOD übersteigen könnte.

Als Entschädigung für die geschäftliche Nutzung eines privaten Gerätes erscheint insgesamt die *Ver einbarung einer monatlichen Pauschalentschädigung*

(Art. 327a Abs. 2 OR) als sinnvoll<sup>28</sup>. Die Pauschalentschädigung muss die durchschnittlichen, effektiven Auslagen tatsächlich decken<sup>29</sup>. Im Sinne der Transparenz und um sicherzustellen, dass zwingend zu ersetzende notwendige Auslagen gemäss Art. 327a Abs. 1 OR abgegolten werden<sup>30</sup>, sind die betreffenden Kostenpositionen einzeln aufzuführen. Fehlen genaue Zahlen (aufgrund der zuvor umschriebenen Erhebungsschwierigkeiten), sollte eine solche Entschädigung den Arbeitnehmer tendenziell begünstigen, um Rechtsstreitigkeiten vorzubeugen. Einerseits kann dadurch eine aufwändige Detailprüfung der Verbindungskosten unterbleiben, andererseits kann dadurch ein Anreiz zur Teilnahme am BYOD-Programm geschaffen werden<sup>31</sup>.

### 3. Haftpflichtrechtliche Fragen bei BYOD

#### a) Haftung des Arbeitgebers

Eine Haftung des Arbeitgebers für private Geräte, die auch geschäftlichen Zwecken dienen, ist aufgrund verschiedener Anspruchsgrundlagen denkbar (nachfolgend aa.). Dabei stellen sich viele Fragen (nachfolgend bb.).

#### aa) Anspruchsgrundlagen einer Haftung des Arbeitgebers

Zunächst hat der Arbeitgeber im Rahmen seiner *Fürsorgepflicht* (Art. 328 OR) die notwendigen Massnahmen zum Schutz des Eigentums des Arbeitnehmers am Arbeitsplatz zu treffen<sup>32</sup>. Zu denken ist dabei z.B. an verschliessbare Aufbewahrungsmöglichkeiten für BYOD-Geräte. Allerdings fliesst aus Art. 328 OR keine Garantiepflcht des Arbeitgebers. Wird z.B. ein Gerät des Arbeitnehmers trotz angemessener Schutz-

<sup>26</sup> Ebenso Birkhäuser/Hadorn (Fn. 12), S. 202; Fanti (Fn. 1), S. 177 f. Anders Mathys (Fn. 1), S. 2, für die Amortisationskosten (da die Lebensdauer der Geräte nicht vom Ausmass der geschäftlichen Nutzung abhängt). Einige Autoren (Reutter/Klaus (Fn. 13), S. 162; Michèle Stutz/Noemi Valloni, Social Media im Arbeitsrecht, in: Oliver Staffelbach/Claudia Keller (Hrsg.), Social Media und Recht für Unternehmen, S. 159 ff., S. 178 f.) knüpfen diesbezüglich an Art. 327b OR an, welcher Motorfahrzeuge betrifft. Nach unserer Auffassung scheint aufgrund der unterschiedlichen Eigenschaften von elektronischen Geräten und Fahrzeugen der direkte Weg für eine Entschädigungspflicht über Art. 327a OR näher zu liegen, als die analoge Anwendung von Art. 327b OR. Im Ergebnis führen beide Wege jedoch zum selben Resultat.

<sup>27</sup> Mathys (Fn. 1), S. 2.

<sup>28</sup> Rehbindler/Stöckli (Fn. 25), Art. 327a N 6; Philippe Carruzzo, Le contrat individuel de travail, Commentaire des articles 319 à 341 du Code des obligations, Zürich 2009, Art. 327a N 4.

<sup>29</sup> BGE 131 III 439 E. 5.3.2; Reutter/Klaus (Fn. 13), S. 162; vgl. die Gedanken zum Home Office: Romina Carcagni Roesler, Home Office, ArbR 2014, S. 71 ff., S. 89 f.

<sup>30</sup> Birkhäuser/Hadorn (Fn. 12), S. 201 ff.

<sup>31</sup> So Mathys (Fn. 1), S. 2.

<sup>32</sup> Streiff/von Kaenel/Rudolph (Fn. 24), Art. 328 N 13, m.w.H.

massnahmen beschädigt oder gestohlen, kann ein Ersatzanspruch nicht auf Art. 328 OR gestützt werden<sup>33</sup>.

Falls das BYOD-Gerät während der geschäftlichen Verwendung beschädigt, zerstört oder gestohlen wird, kann eine Ersatzpflicht des Arbeitgebers auch deshalb in Frage kommen, *weil der Arbeitgeber das Arbeitsgerät bereitzustellen hat*, sofern nichts anderes vereinbart oder üblich ist (Art. 327 Abs. 1 OR)<sup>34</sup>. Wäre in derselben Situation ein vom Arbeitgeber bereitgestelltes Gerät betroffen, müsste dieser den Schaden auch in vollem Umfang selbst tragen. Gleichzeitig führen einige Autoren eine analoge Anwendung der Praxis zu Art. 327b OR ins Feld<sup>35</sup>, wonach der Arbeitgeber für Unfälle mit Privatfahrzeugen während der geschäftlichen Nutzung haftet<sup>36</sup>. Zudem hat der Arbeitgeber dem Arbeitnehmer nach Art. 327a OR alle durch die Ausführung der Arbeit notwendigen Auslagen zu ersetzen<sup>37</sup>.

Arbeitgeber und Arbeitnehmer können sich im Voraus über eine anteilmässige Entschädigung für Reparaturkosten und Kosten eines Ersatzgerätes (Abgeltung des Schaden-, Diebstahl- und Verlustrisikos) als Teil einer monatlichen Pauschalentschädigung *vertraglich einigen*. Diese Entschädigung ist nach objektiven Kriterien wie durchschnittliche Lebensdauer des BYOD-Gerätes, Abschreibungsgrundsätze, Höhe einer Versicherungsprämie für das Gerät, etc., zu bemessen. Es ist zu beachten, dass eine zu geringe Entschädigung eine Verletzung der einseitig zwingenden Bestimmung von Art. 327a OR zur Folge haben kann (Art. 362 Abs. 1 OR, s. oben III.2.).

## bb) Konkrete Fragen

Selbst wenn eine Anspruchsgrundlage erfüllt ist, stellen sich bei der Haftung des Arbeitgebers viele verschiedene Fragen:

### (1) *Hat der Arbeitgeber beim vollständigen Untergang das Gerät selbst (Realersatz) oder den Geldwert des BYOD-Gerätes zu ersetzen?*

Im analog anwendbaren Schadensersatzrecht gilt grundsätzlich die Geldzahlung als massgebliche Entschädigungsart<sup>38</sup>. Eine Abweichung von diesem Grundsatz lässt sich nicht mit der Teilnahme des Arbeitnehmers an einem BYOD-Programm begründen. Denn dem Arbeitnehmer steht es frei, am Programm teilzunehmen (s. oben III.1.). Er allein entscheidet, wie er eine Ersatzzahlung verwendet<sup>39</sup>. Folglich muss sich der Arbeitnehmer eine Einschränkung durch Realersatz nicht gefallen lassen. Vorbehalten bleiben abweichende Parteivereinbarungen.

### (2) *Darf der Arbeitgeber bei einer teilweisen Beschädigung des BYOD-Gerätes bzw. der Software (z.B. durch einen Virenbefall durch ein geschäftliches E-Mail) Realersatz (z.B. Wiederherstellung durch die IT-Abteilung) leisten?*

Im Schadensersatzrecht gilt, dass Geschädigte nicht zu Realersatz gezwungen werden dürfen, es sei denn, die Naturalrestitution sei zumutbar und die preisgünstigste Lösung<sup>40</sup>. In Fällen, in denen die IT-Abteilung des Arbeitgebers in der Lage ist, das BYOD-Gerät zu reparieren, dürfte kaum etwas gegen einen solchen Realersatz sprechen. Muss der Arbeitgeber für die Reparatur einen Dritten (z.B. das Gerät zur Reparatur an den Hersteller einschicken) beiziehen (indirekter Realersatz), ist das Einverständnis des Arbeitnehmers notwendig<sup>41</sup>. Es ist dem Arbeitnehmer zu empfehlen, vor der Abgabe eines BYOD-Gerätes Vorkehrungen zu treffen, um einem Missbrauch seiner persönlichen Daten vorzubeugen. Dafür kommt z.B. ein Backup mit anschliessen-

<sup>33</sup> Wolfgang Portmann/Roger Rudolph, Basler Kommentar, Obligationenrecht I, Art. 1–529, 6. Aufl., Basel 2015, Art. 328 N 48; Streiff/von Kaenel/Rudolph (Fn. 24), Art. 328 N 13, m.w.H.

<sup>34</sup> Ähnlich zum deutschen Recht Zöll/Kielkowski (Fn. 6), S. 2627.

<sup>35</sup> Fanti (Fn. 1), S. 178; Reutter/Klaus (Fn. 13), S. 161; Mathys (Fn. 1), S. 2 f., der für die Beantwortung der Haftungsfrage zusätzlich Geräteart und den Verwendungszweck einbezieht.

<sup>36</sup> Weiterführend zu Unfällen des Arbeitnehmers auf Geschäftsfahrt Streiff/von Kaenel/Rudolph (Fn. 24), Art. 327b N 4.

<sup>37</sup> Weiterführend Streiff/von Kaenel/Rudolph (Fn. 24), Art. 327a N 1 ff.

<sup>38</sup> Roland Brehm, Berner Kommentar, Die Entstehung durch unerlaubte Handlungen, Art. 41–61 OR, Schweizerisches Zivilgesetzbuch, Das Obligationenrecht, 4. Aufl., Bern 2013, Art. 43 N 5.

<sup>39</sup> BK OR-Brehm (Fn. 38), Art. 43 N 6.

<sup>40</sup> BK OR-Brehm (Fn. 38), Art. 43 N 19.

<sup>41</sup> Vgl. BK OR-Brehm (Fn. 38), Art. 43 N 19.

der Löschung der privaten Daten auf dem Gerät in Frage.

- (3) *Welcher Wert ist bei einem vollständigen Untergang des Gerätes zu ersetzen?*

Da es sich bei BYOD-Geräten in der Regel um nicht wertbeständige Sachen handelt, ist nur der Gebrauchtwert (sog. Zeitwert) zu ersetzen. Das bedeutet, dass der Preis für ein vergleichbares Gerät auf dem Occasionsmarkt vom Arbeitgeber zu ersetzen ist<sup>42</sup>.

- (4) *Von welchem Wert ist für den Ersatzanspruch des Arbeitnehmers auszugehen, falls er ein deutlich teureres Gerät als notwendig verwendet (z.B. ein vergoldetes Smartphone)?*

Sofern den Arbeitgeber kein Verschulden trifft, gründet der Ersatzanspruch des Arbeitnehmers auf dem Umstand, dass der Arbeitgeber bei einem Schadensfall auch ein von ihm zur Verfügung gestelltes Arbeitsgerät zu ersetzen oder zu reparieren hätte (vgl. Art. 327 Abs. 1 OR, s. oben III.3.a.aa.). Vor diesem Hintergrund wäre es stossend, müsste der Arbeitgeber einen Wert ersetzen, der deutlich über dem eines üblichen Arbeitsgerätes liegt. Demzufolge beschränkt sich der Ersatzanspruch auf ein durchschnittliches, für die Arbeitserledigung benötigtes Gerät. Als Richtschnur können Geräte dienen, die der Arbeitgeber den nicht am BYOD-Programm beteiligten Arbeitnehmern zur Verfügung stellt. Vorbehalten sind ausdrückliche Parteivereinbarungen.

- (5) *Hat der Arbeitgeber bei jedem Schaden an einem BYOD-Gerät einzustehen?*

Grundsätzlich ist der Arbeitgeber nur für Schäden ersatzpflichtig, die im Rahmen der Erbringung der Arbeitsleistung des Arbeitnehmers entstehen<sup>43</sup>. Kein Zuordnungsproblem besteht bei Schäden, die aus der Verantwortlichkeitssphäre des Arbeitgebers herrühren. Zu denken ist dabei z.B. an Schadsoftware, die sich über einen Geschäftsserver verbreitet. Bei anderen Schäden wird relevant, ob das Gerät während der Schädigung privat oder geschäftlich genutzt wurde. Da ein BYOD-Gerät auch ausserhalb des Arbeitsortes geschäftlich genutzt werden kann, ist diese

Unterscheidung problematisch. Ein Lösungsansatz ist, darauf abzustellen, ob die Schädigung während einer Tätigkeit erfolgt, die als Arbeitszeit zu betrachten ist (s. unten III.6.). Für Schäden während der Arbeitszeit hat der Arbeitgeber einzustehen<sup>44</sup>.

- (6) *Hat der Arbeitgeber für Schäden einzustehen, die der Arbeitnehmer am eigenen BYOD-Gerät (teilweise) selbst verschuldet?*

Für Schäden, die ein Arbeitnehmer seinem BYOD-Gerät während der Arbeitszeit selbst zufügt, kommt Art. 321e OR analog zur Anwendung<sup>45</sup>. Somit ist im Einzelfall zu entscheiden, nach welchem Mass der Sorgfalt (Art. 321e Abs. 2 OR) der Arbeitnehmer selbst für den Schaden einzustehen hat<sup>46</sup>. Demzufolge kann der Arbeitgeber verpflichtet sein, zumindest einen Teil des während der Arbeitszeit entstandenen Schadens am BYOD-Gerät zu tragen<sup>47</sup>. Neben der absichtlichen Verursachung eines Schadens durch den Arbeitnehmer können leichte, mittlere und grobe Fahrlässigkeit unterschieden werden<sup>48</sup>. Bei grober Fahrlässigkeit werden elementare Vorsichtspflichten missachtet<sup>49</sup>. Zu denken ist z.B. an einen Arbeitnehmer, der sein BYOD-Gerät während eines Toilettenganges in einem belebten Restaurant bewusst unbeaufsichtigt und ungesichert am Tisch zurücklässt. Bei Schäden aus Unachtsamkeit kann von leichter Fahrlässigkeit gesprochen werden. Das kann z.B. der Fall sein, falls dem Arbeitnehmer das BYOD-Gerät beim Bezahlen am Kiosk unbemerkt aus der Tasche rutscht und dadurch verloren geht. Für Fälle, die zwischen grober und leichter Fahrlässigkeit liegen, existiert die Kategorie der mittleren Fahrlässigkeit. Sie findet dort Anwendung, wo Vorsichtspflichten missachtet werden, die nicht als elementar zu klas-

<sup>42</sup> Heinrich Honsell/Bernhard Isenring/Martin A. Kessler, Schweizerisches Haftpflichtrecht, 5. Aufl., Zürich 2013, § 8 Rz. 47.

<sup>43</sup> Fanti (Fn. 1), S. 178; Reutter/Klaus (Fn. 13), S. 178.

<sup>44</sup> Ähnlich Fanti (Fn. 1), S. 178, der argumentiert, dass der Arbeitgeber für einen Schaden am BYOD-Gerät während der Ferien nicht haftet.

<sup>45</sup> Vgl. BSK OR I-Portmann/Rudolph (Fn. 33), Art. 321e N 24.

<sup>46</sup> S. zu den Gründen, die eine Reduktion bzw. einen Wegfall der Schadenstragung durch den Arbeitnehmer bewirken, BSK OR I-Portmann/Rudolph (Fn. 33), Art. 321e N 5 ff.

<sup>47</sup> Vgl. auch Fanti (Fn. 1), S. 179, der insbesondere auf die Beweisprobleme des Arbeitnehmers hinweist.

<sup>48</sup> BGE 100 II 332 E. 3.

<sup>49</sup> BGE 111 II 90 E. 1a.

sifizieren sind<sup>50</sup>. Als Faustregel gilt, dass bei grober Fahrlässigkeit bis zu einer Schadenshöhe von drei Monatslöhnen grundsätzlich keine Haftungsreduktion stattfindet. Bei mittlerer Fahrlässigkeit soll der Arbeitnehmer für zwei Drittel des Schadens bis maximal zu zwei Monatslöhnen haften. Leichte Fahrlässigkeit soll die Haftung bis zur Hälfte des Schadens und maximal bis zu einem Monatslohn zur Folge haben<sup>51</sup>. Die Haftung des Arbeitnehmers nach Art. 321e OR kann durch Parteiabreden nicht verschärft werden<sup>52</sup>. Demzufolge wäre eine Vereinbarung, wonach der Arbeitnehmer für jeden Schaden des BYOD-Gerätes vollen Ersatz zu leisten hat, unzulässig.

(7) *Hat der Arbeitnehmer Anspruch auf ein Ersatzgerät während der Reparatur?*

Zur Erledigung der geschäftlichen Aufgaben muss der Arbeitgeber den Arbeitnehmer mit einem Ersatzgerät ausstatten (Art. 327 Abs. 1 OR), unabhängig davon, ob der Schaden am BYOD-Gerät privat oder geschäftlich verursacht worden ist (s. oben III.1.) – sofern das Mitbringen privater Arbeitsgeräte nicht branchenüblich ist oder eine abweichende Parteivereinbarung besteht. Ob der Arbeitnehmer auch Anspruch auf die private Nutzung eines Ersatzgerätes hat, ist im Einzelfall zu entscheiden. Ist der Schaden des BYOD-Gerätes der privaten Sphäre des Arbeitnehmers zuzuteilen, hat der Arbeitnehmer keinen Anspruch auf die private Nutzung eines Ersatzgerätes. Bei Schäden, die während der Arbeitszeit entstehen, ist im Einzelfall zu entscheiden, ob der Arbeitnehmer tatsächlich ein privates Ersatzgerät benötigt. Dies dürfte bei einem Smartphone der Fall sein<sup>53</sup>, bei einem Tablet, das privat einzig zur Freizeitgestaltung (z.B. zum Spielen) genutzt wird, wohl nicht<sup>54</sup>.

Dem Arbeitgeber ist dringend zu empfehlen, die Entschädigung bei einem Schadensfall des BYOD-

Gerätes vorgängig mit dem Arbeitnehmer zu regeln. Diese Regelung sollte zudem in Zusammenhang mit einer umfassenden BYOD-Richtlinie stehen (s. unten IV.).

#### b) Haftung des Arbeitnehmers

Auch der Arbeitnehmer kann für Schäden durch sein BYOD-Gerät verantwortlich sein, z.B. wenn sein Gerät das Netzwerk des Arbeitgebers mit Schadsoftware infiziert oder Dritte über sein Gerät Zugang zu schützenswerten Daten des Arbeitgebers erhalten<sup>55</sup>. Gemäss Art. 321e Abs. 1 OR ist der Arbeitnehmer für Schäden verantwortlich, die er dem Arbeitgeber absichtlich oder fahrlässig verschuldet. Für die Beurteilung des Verschuldens des Arbeitnehmers im Einzelfall ist der Sorgfaltsmassstab von Art. 321e Abs. 2 OR anzuwenden<sup>56</sup>. Dabei ist unter anderem der Bildungsgrad bzw. die Fachkenntnis des Arbeitnehmers zu berücksichtigen (Art. 321e Abs. 2 OR). Eine vorgängige Instruktion des Arbeitgebers über das Verwenden von BYOD-Richtlinien kann haftungsverschärfend wirken<sup>57</sup>. Somit ist der Arbeitnehmer nicht nur aus Gründen der Prävention<sup>58</sup> beim Einsatz von BYOD vorgängig umfassend über die geltende BYOD-Richtlinie zu informieren.

#### 4. Datenschutzrechtliches Minenfeld

Eines der grössten Probleme beim BYOD ist der Datenschutz, und zwar sowohl aus Sicht des Arbeitgebers wie auch aus Sicht des Arbeitnehmers. Um Sicherheits- und Reputationsrisiken einzudämmen, kann es für den Arbeitgeber essentiell sein, *Daten auf dem BYOD-Gerät zu bearbeiten*, z.B. zu durchsuchen oder zu löschen<sup>59</sup>. Bei der Bearbeitung von Personendaten ist das Datenschutzgesetz (DSG) zu beachten. Die Daten auf einem BYOD-Gerät sind als *Personendaten* im Sinne von Art. 2 Abs. 1 lit. a DSG

<sup>50</sup> Zur Klassifizierung der Fahrlässigkeit s. *Streiff/von Kaenel/Rudolph* (Fn. 24), Art. 321e N 2, m.w.H. und *Stefanie Meier-Gubser*, Haftung des Arbeitnehmers, TREX 2012, S. 292 ff., S. 293.

<sup>51</sup> *Meier-Gubser* (Fn. 50), S. 293.

<sup>52</sup> *Streiff/von Kaenel/Rudolph* (Fn. 24), Art. 321e N 5.

<sup>53</sup> A. M. *Mathys* (Fn. 1), S. 2, der eine Ersatzpflicht bei einem privaten Mobiltelefon grundsätzlich ablehnt.

<sup>54</sup> Vgl. dazu die Praxis im allgemeinen Schadensrecht in *Honsell/Isenring/Kessler* (Fn. 42), § 8 Rz. 54, m.w.H.

<sup>55</sup> *Mathys* (Fn. 1), S. 3.

<sup>56</sup> BSK OR I-*Portmann/Rudolph* (Fn. 33), Art. 321e N 3 ff.

<sup>57</sup> *Mathys* (Fn. 1), S. 3.

<sup>58</sup> *Fanti* (Fn. 1), S. 179.

<sup>59</sup> Vgl. zu Sicherheitsrisiken *Roland Portmann*, Private Smartphones im Geschäftsumfeld, *digma* 2012, S. 42 ff., S. 43; *Andreas Kohne/Sonja Ringleb/Cengizhan Yücel*, Bring your own Device: Einsatz von privaten Endgeräten im beruflichen Umfeld – Chancen, Risiken und Möglichkeiten, Wiesbaden 2015, S. 133 ff.

zu qualifizieren, sofern sie einen Arbeitnehmerbezug aufweisen<sup>60</sup>.

Eines der grundsätzlichen Bedenken von Arbeitnehmern gegenüber BYOD könnte sein, dass trotz einer Regelung der Bearbeitung privater Daten in einer BYOD-Richtlinie ein Übergriff des Arbeitgebers auf private Daten zu unzulässigen *Überwachungszwecken* im Bereich des technisch Möglichen liegt. Die Gefahr einer heimlichen Überwachung stellt sich aber nicht nur bei BYOD, sondern allgemein bei E-Mail und Internet<sup>61</sup>.

Für eine Datenbearbeitung auf dem BYOD-Gerät ist ein *Rechtfertigungsgrund* notwendig. Art. 328b OR schränkt im Arbeitsverhältnis die zulässigen Datenkategorien und Bearbeitungszwecke ein: Gemäss Art. 328b OR darf der Arbeitgeber nur Daten über den Arbeitnehmer bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind.

Der Bearbeitung geschäftlicher Personendaten (z.B. das Durchsuchen oder Löschen geschäftlicher E-Mails) kann der Arbeitnehmer in einer generellen *Einwilligung*, z.B. im Rahmen einer BYOD-Vereinbarung, zustimmen<sup>62</sup>. Eine stillschweigende Einwilligung des Arbeitnehmers wird bei geschäftlichen Daten vermutet, die der Arbeitnehmer mit anderen Mitarbeitern des Arbeitgebers teilt (vgl. Art. 12 Abs. 3 DSG), z.B. auf einem für mehrere Arbeitnehmer zugänglichen Laufwerk gespeicherte Dokumente. Demgegenüber bedarf es aufgrund der einseitigen Unabänderlichkeit zum Nachteil des Arbeitnehmers von Art. 328b OR (Art. 362 Abs. 1 OR) für eine Bearbeitung privater Daten bei BYOD strengerer Anforderungen. Sie ist nur möglich, wenn sie im Einzelfall, und wenn sie (auch) im Interesse des Arbeitnehmers erfolgt<sup>63</sup>.

Anstelle einer Einwilligung kann ein *überwiegendes (privates oder öffentliches) Interesse des Arbeitgebers* treten (Art. 13 Abs. 1 DSG). Die Frage, wann ein überwiegendes Interesse des Arbeitgebers zur Bearbeitung privater Daten des Arbeitnehmers gegeben sein könnte, ist von Fall zu Fall zu entscheiden und erfordert eine Güterabwägung<sup>64</sup>. Im Fall des Verlusts des Gerätes oder bei Beendigung des Arbeitsverhältnisses kann beispielsweise eine Löschung der Daten im überwiegenden Interesse des Arbeitgebers liegen<sup>65</sup>, sofern dies z.B. aus Sicherheitsgründen notwendig sein sollte. Wann genau der Arbeitgeber Daten löschen darf, ist eine sehr heikle Frage. Ein überwiegendes Interesse könnte ebenfalls bei der Durchsuchung von Daten infolge eines vermuteten schweren Missbrauchs (z.B. Straftat gegen den Arbeitgeber) vorliegen<sup>66</sup>.

Jede Massnahme des Arbeitgebers steht jedoch unter der Bedingung der *Verhältnismässigkeit* (Art. 4 Abs. 2 DSG). Ebenso muss der Arbeitnehmer bei einer allgemeinen Einwilligung (z.B. im Rahmen einer BYOD-Vereinbarung) informiert worden sein, in welchen Fällen Daten bearbeitet bzw. gelöscht werden können (Ersichtlichkeit und Erkennbarkeit gemäss Art. 4 Abs. 2 und 3 DSG), also z.B. bei Verlust des Gerätes oder bei Beendigung des Arbeitsverhältnisses. Gleichzeitig ist dem Arbeitnehmer die Datenbearbeitung anzukündigen, sofern kein berechtigtes Interesse (z.B. an einer verdeckten Untersuchung) entgegensteht (vgl. Prinzip von Treu und Glauben in Art. 4 Abs. 2 DSG)<sup>67</sup>.

Es gibt mehrere BYOD-spezifische datenschutzrechtliche Problemfelder:

- (1) Die Unterscheidung zwischen geschäftlichen und privaten Daten wird in der Praxis bei BYOD sehr schwierig sein. Wenn aber geschäftliche und private Daten kaum mehr zu unterscheiden sind, so kann z.B. die Überprüfung eines Missbrauchs- und Betrugsverdachts kompliziert sein. Wie ist z.B. bei BYOD ein Verbindungsnachweis über Telefongespräche des Arbeitnehmers handzuhaben? Was sind die Anforderungen an einen Ver-

<sup>60</sup> Birkhäuser/Hadorn (Fn. 12), S. 203 m.w.H.

<sup>61</sup> S. zur flächendeckenden Überwachung in grossen Unternehmen: Zoé Baches, Wie sich Firmen vor eigenen Mitarbeitern schützen, NZZ Online 11.10.2016, <<http://www.nzz.ch/wirtschaft/unternehmen/wirtschaftskriminalitaet-firmen-schuetzen-sich-vor-den-eigenen-mitarbeitern-ld.121315>>

<sup>62</sup> Birkhäuser/Hadorn (Fn. 12), S. 203; David Rosenthal, in: David Rosenthal/Yvonne Jöhri (Hrsg.), Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 328b OR N 41; Streiff/von Kaenel/Rudolph (Fn. 24), Art. 328b N 6.

<sup>63</sup> Mathys (Fn. 1), S. 3; Birkhäuser/Hadorn (Fn. 12), S. 203; Rosenthal (Fn. 62), Art. 328b OR N 14.

<sup>64</sup> Mathys (Fn. 1), S. 3.

<sup>65</sup> Mathys (Fn. 1), S. 3; Birkhäuser/Hadorn (Fn. 12), S. 205. Anders Fanti (Fn. 1), S. 171 («qu'avec son accord formel, préalable et éclairé»).

<sup>66</sup> Birkhäuser/Hadorn (Fn. 12), S. 205.

<sup>67</sup> S. ausführlich Fanti (Fn. 1), S. 183 ff.

*bindungsnachweis*, der auch private Verbindungen erfasst? Oder ein anderes Beispiel: In gewissen Branchen ist es (teilweise aus regulatorischen Gründen) üblich, dass sämtliche Telefongespräche automatisch aufgenommen werden, z.B. die Gespräche von Kundenberatern. Wenn nun öfters von einem BYOD-Gerät aus telefoniert wird, stellt sich die Frage, ob dann letztlich zu einem erheblichen Teil auch private Anrufe aufgenommen werden.

- (2) Eine Sicherheitsmassnahme des Arbeitgebers kann der *Einzug des BYOD-Gerätes* durch den Arbeitgeber sein, entweder mit oder ohne Bearbeitung der darauf befindlichen Daten. Der Arbeitgeber ist zum Einzug berechtigt, falls der Arbeitnehmer in einer allgemeinen BYOD-Vereinbarung oder im Einzelfall zugestimmt hat<sup>68</sup>. Auch hier kann anstelle einer Einwilligung ein überwiegendes Interesse des Arbeitgebers treten, wobei die notwendige Güterabwägung schwierig sein kann, und die Frage, wann genau der Arbeitgeber das Gerät einziehen kann, heikel ist.

Ein Einzug des BYOD-Gerätes kann wichtig sein. Man denke z.B. an eine *Freistellung* bei einem Investment Bank Trader. Bei einem BYOD-Gerät können der Einzug und der Zugriff zwecks einer IT-Überprüfung des Geräts problematisch sein. Zudem besteht die Gefahr, dass der Arbeitnehmer Daten in einem privaten Backup speichert, auf das der Arbeitgeber keinen Zugriff hat. Je nach Branche, wenn die Datensicherheit sehr wichtig ist, empfiehlt es sich deshalb unseres Erachtens, von BYOD Abstand zu nehmen. Wird ein BYOD-Gerät eingezogen, so kann der Arbeitgeber verpflichtet sein, den Arbeitnehmer dafür zu entschädigen oder für einen gleichwertigen Ersatz zu sorgen. Eine solche Pflicht kann für die geschäftliche Nutzung aus Art. 327 OR, wonach der Arbeitgeber verpflichtet ist, die notwendigen Arbeitsgeräte zur Verfügung zu stellen, und für die private Verwendung aus Art. 328 Abs. 1 OR, der Fürsorgepflicht des Arbeitgebers, abgeleitet werden. Die praktische Umsetzung im Einzelfall kann allerdings Probleme verursachen, insbesondere wenn die ursprünglich private Nummer des Arbeitnehmers «eingezogen» wird.

- (3) Handelt es sich beim BYOD-Gerät um ein Mobiltelefon, wird die private Telefonnummer oft in einem *Geschäftstelefonverzeichnis* hinterlegt. Das kann für Arbeitnehmer und Arbeitgeber Nachteile haben. Insbesondere bei grossen Unternehmen verliert der Arbeitnehmer die Kontrolle darüber, wer Zugang zu seiner privaten Nummer hat, wodurch Persönlichkeitsverletzungen Vorschub geleistet wird. Gleichzeitig verliert der Arbeitgeber die Kontrolle über Teile der Kommunikationsinfrastruktur. Tritt ein Arbeitnehmer aus dem Unternehmen des Arbeitgebers aus, können Kunden, Geschäftspartner und Mitarbeiter ungehindert weiterhin mit dem ausgetretenen Arbeitnehmer kommunizieren – im Zweifelsfall ohne den Arbeitgeberwechsel des Arbeitnehmers zu bemerken. Dadurch entsteht Missbrauchspotential z.B. für unzulässige Kundenabwerbungen.

## 5. Regelungskompetenz des Arbeitgebers

Die arbeitgeberseitige *Regelung der Nutzung privater Geräte* ist problematisch<sup>69</sup>. Anders als bei der Nutzung unternehmenseigener Infrastruktur sind die Geräte bei BYOD ja im Eigentum der Arbeitnehmer. Grundsätzlich können Arbeitgeber ihren Arbeitnehmern die private Nutzung ihres Geräts nicht vorschreiben, und es besteht keine Regelungsbefugnis des Arbeitgebers, solange die Nutzung keine Auswirkungen auf das Arbeitsverhältnis hat<sup>70</sup>.

Bei BYOD müssen *Verhaltensanweisungen* an die Arbeitnehmer sowie *technische Massnahmen*, die eine bestimmte Nutzung erzwingen oder vorschreiben (wie Passwortvorgaben, automatische Lockscreens, oder Installationsverbote von Apps aus inoffiziellen Quellen), zulässig sein, wenn sie als notwendig und verhältnismässig eingestuft werden, und wenn sie

<sup>68</sup> Zu Löschung, Durchsuchung oder Beschlagnahmung von BYOD-Geräten s. *Birkhäuser/Hadorn* (Fn. 12), S. 202 ff.

<sup>69</sup> S. dazu die Tabelle 3 von *Isabelle Wildhaber/Silvio Hänsenberger*, Kündigung wegen Nutzung von Social Media – wenn Arbeit und Privatleben kollidieren, in: *Recht im digitalen Zeitalter*, FS Schweizerischer Juristentag 2015, St. Gallen 2015, S. 399 ff., S. 424 ff., S. 425.

<sup>70</sup> *Wildhaber/Hänsenberger* (Fn. 17), S. 337 ff., *Wildhaber/Hänsenberger*, *Recht im digitalen Zeitalter* (Fn. 69), S. 425; *Isabelle Wildhaber/Silvio Hänsenberger*, Kündigungsfälle Social Media, *sui-generis* 2015, S. 77 ff., S. 87 ff. auf <<http://sui-generis.ch/14>>.

zu Zwecken der IT-Sicherheit des Arbeitgebers erfolgen<sup>71</sup>.

## 6. Arbeitsgesetz und BYOD

Das Konzept des BYOD begünstigt den Trend zu einer «Entgrenzung» der Arbeit im Sinne der Aufhebung klarer Grenzen zwischen Wohn- und Arbeitsort und zwischen Arbeits- und Freizeit<sup>72</sup>. Durch mobile Geräte wie Laptops, Tablets und Smartphones kann die Grenze zwischen Arbeitszeit und Freizeit verwischt werden. Die ständige Erreichbarkeit kann im Konflikt mit den Bestimmungen zur zulässigen Höchstarbeitszeit und zur Nacht- und Sonntagsarbeit, zum Ferienbezug und zur Entlohnung stehen<sup>73</sup>. Das Problem der ständigen Erreichbarkeit besteht aber nicht nur bei BYOD-Geräten, sondern auch dann, wenn die Geräte vom Arbeitgeber stammen. Die «Entgrenzung der Arbeit» wird allerdings bei BYOD erhöht, wenn ansonsten ein Zugriff auf E-Mail ausserhalb der festen Arbeitszeiten nicht möglich wäre.

Auf der Hand liegt, dass die tatsächliche Einsatzzeit, während der der Arbeitnehmer geschäftliche Aufgaben ausserhalb seines Arbeitsplatzes erledigt (z.B. E-Mails beantworten, Anrufe entgegen nehmen etc.), als *Arbeitszeit* gilt. Verhindert die Notwendigkeit zur ständigen geschäftlichen Erreichbarkeit zudem eine sinnvolle Freizeitgestaltung und Erholung, ist diese Zeit als Arbeitszeit zu taxieren. Dies gilt in der Regel dann nicht, wenn es sich um die blossere Bereitschaft handelt, bei Gelegenheit geschäftliche Aufgaben zu erledigen und dadurch keine weitergehende Einschränkung der Freizeitgestaltung entsteht<sup>74</sup>. Wird der Erholungszweck der Ferien (Art. 329a OR) durch die Erledigung geschäftlicher Aufgaben untergraben, hat der Arbeitgeber in schwerwiegenden Fällen den Ferienanspruch erneut zu gewähren<sup>75</sup>.

In den zuvor umschriebenen Fällen kann eine *Vernachlässigung der Fürsorgepflicht* (Art. 328 OR) des

Arbeitgebers erblickt werden, welche im Anwendungsbereich des Arbeitsgesetzes in Art. 6 ArG sowie in der ArGV 3 konkretisiert wird<sup>76</sup>. Demnach hat der Arbeitgeber aktiv Massnahmen zum Schutz der Arbeitnehmer zu treffen (Art. 328 Abs. 2 OR sowie Art. 6 Abs. 1–2 ArG), insbesondere vor Gesundheitsgefährdung durch Überbeanspruchung (Art. 6 Abs. 2 ArG). Solche Massnahmen können die Information und Sensibilisierung der Arbeitnehmer sein oder aber auch technische Vorkehrungen, welche bewirken, dass geschäftliche Daten (z.B. E-Mails und Telefonanrufe) ausserhalb der Arbeitszeit und während den Ferien nicht an das BYOD-Gerät weitergeleitet werden.

## IV. BYOD-Richtlinien

BYOD ist in vielen Unternehmen längst Realität. Entweder wird BYOD eingeführt oder aber faktisch geduldet. Die geschäftsmässige Nutzung privater Geräte ist dabei in den meisten Fällen nicht explizit geregelt. Aufgrund der genannten rechtlichen Unklarheiten ist aber eine *Regelung von BYOD zu empfehlen*. BYOD-Richtlinien sollten Gegenstand einer Vereinbarung mit dem Arbeitnehmer sein, in Ergänzung zu einem Internet-/E-Mail- oder Social Media-Reglement. Eine Implementierung von BYOD setzt zwingend eine *vertragliche Vereinbarung* zwischen Arbeitgeber und Arbeitnehmer voraus<sup>77</sup>.

Um Datenschutz- und Sicherheitsrisiken zu minimieren, ist dabei zu beachten, *geschäftliche von privaten Daten (sowohl technisch als auch logisch) strikt zu trennen*<sup>78</sup>. Dazu empfiehlt sich eine separate geschäftliche Softwareumgebung, indem Daten und Programme in der Cloud oder mittels sog. Container Apps und anderen Visualisierungstechniken (bei denen praktisch auf dem Server des Arbeitgebers gearbeitet wird) separiert von den privaten Daten des Arbeitnehmers zur Verfügung gestellt werden<sup>79</sup>.

<sup>71</sup> So Mathys (Fn. 1), S. 3.

<sup>72</sup> Wolfgang Däubler, Entgrenzung der Arbeit – Ein Problem des Arbeitsrechts?, Soziales Recht 2/2014, S. 45 ff.

<sup>73</sup> Weiterführend Adrian von Kaenel, Die ständige Erreichbarkeit des Arbeitnehmers, ARV 2009, S. 1 ff.

<sup>74</sup> Roger Rudolph/Adrian von Kaenel, Fokus Arbeitsrecht. Aktuelle Fragen zur Arbeitszeit, TREX 2014, S. 166 ff., S. 170.

<sup>75</sup> Reutter/Klaus (Fn. 13), S. 163.

<sup>76</sup> S. Letsch (Fn. 13), N 112 f., 123 ff. und N 133 ff.

<sup>77</sup> Fanti (Fn. 1), S. 200; Reutter/Klaus (Fn. 13), S. 165; Nicole Beranek Zanon, Bring your own device (BYOD) aus rechtlicher Sicht, Jusletter IT vom 12.9.2012, Rz. 51 f. Formulierungsbeispiele in Birkhäuser/Hadorn (Fn. 12), S. 206; Stutz/Valloni (Fn. 26), S. 185.

<sup>78</sup> EDÖB (Fn. 15).

<sup>79</sup> Z.B. die Software «BizzTrust», welche durch das Fraunhofer-Institut für Sichere Informationstechnologie (SIT) entwickelt wurde, s. <<https://www.sit.fraunhofer.de/de/bizztrust/>>.

Folgende Punkte sollten geregelt werden. Dabei sind im Einzelfall die untenstehenden Bestimmungen an die Risikotoleranz des Arbeitgebers, Sensibilität der

verarbeiteten Daten und das Benutzerprofil des Arbeitnehmers anzupassen:

| <b>BYOD-Richtlinien<sup>80</sup></b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.                                   | Verbot des Einsatzes privater Geräte zur Erbringung der Arbeitsleistung (BYOD) und/oder der Speicherung geschäftlicher Daten auf privaten Geräten ohne vorgängige Genehmigung durch die als zuständig erklärte Instanz/Person des Arbeitgebers.                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 2.                                   | Ausschliessliche Speicherorte für geschäftliche Daten festlegen. Zur Trennung von geschäftlichen und privaten Daten verpflichten (sofern dies eine durch den Arbeitgeber bereitgestellte Softwarelösung (z.B. «Container») erlaubt).                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 3.                                   | Anweisung, geschäftliche Daten nur mit der durch den Arbeitgeber bereitgestellten Software zu verarbeiten, zu verschlüsseln, zu speichern und zu übermitteln sowie die eingesetzten Geräte mit Passwörtern in einer, vom Arbeitgeber bestimmten, genügenden Qualität zu schützen.<br>Festlegen von Bestimmungen über die Aufbewahrung von Passwörtern.                                                                                                                                                                                                                                                                                                               |
| 4.                                   | Vereinbarung über den Zugriff durch den Arbeitgeber auf die geschäftlichen Daten auf dem Gerät des Arbeitnehmers bzw. den Einzug des Gerätes z.B. zur Geräteüberprüfung, Fernwartung etc. treffen. Festlegen, ob und wie der Arbeitnehmer vorgängig über einen Zugriff des Arbeitgebers informiert wird.<br>Falls private und geschäftliche Daten auf dem privaten Gerät des Arbeitnehmers nicht getrennt sind oder ein Zugriff ausserhalb des geschäftlichen Teils des Gerätes notwendig wird, ist keine globale Einwilligung des Arbeitgebers möglich. Deshalb ist in diesem Fall vor jedem Zugriff des Arbeitgebers die Einwilligung des Arbeitnehmers notwendig. |
| 5.                                   | Verbot, ausschliesslich für private Zwecke lizenzierte Software geschäftlich zu verwenden. Verpflichtung des Arbeitnehmers, die private und geschäftliche Software (inkl. Betriebssystem) regelmässig zu aktualisieren und auf dem neusten Stand zu halten, allenfalls verbunden mit der Pflicht zur Aktivierung automatischer Aktualisierungen.                                                                                                                                                                                                                                                                                                                     |
| 6.                                   | Meldepflicht bei Verlust, Diebstahl, Beschädigung, Befall mit Schadsoftware des Gerätes oder (vermutetem) unbefugtem Zugriff auf das Gerät. Als Anreiz für den Mitarbeiter kann der Arbeitgeber allenfalls ein Ersatzgerät oder Support zur Verfügung stellen.                                                                                                                                                                                                                                                                                                                                                                                                       |
| 7.                                   | Verbot der Vornahme von nicht autorisierten Hardwareveränderungen am Gerät oder nicht autorisierten Veränderungen am Betriebssystem («Jailbreak»/«Rooten» des Geräts).<br>Alle installierten Anwendungen müssen aus offiziellen, vom Entwickler des jeweiligen Betriebssystems autorisierten Quellen entstammen. Es darf kein Code von fragwürdigen Quellen installiert werden. Die Informatikabteilung des Arbeitgebers beurteilt im Einzelfall, ob eine Anwendung vertrauenswürdig ist.                                                                                                                                                                            |
| 8.                                   | Verbot, das Gerät in durch den Arbeitgeber bestimmte Länder mitzuführen (namentlich Länder, deren Einreisebehörden für die Überprüfung von elektronischen Geräten bekannt sind).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 9.                                   | Verpflichtung, das Gerät ausschliesslich an Computer anzuschliessen, welche über einen aktuellen, aktivierten Malware-Schutz verfügen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 10.                                  | Bestimmung, dass E-Mails und andere Korrespondenzen nur von geschäftlichen Konten aus getätigt werden dürfen. Verbot der Verwendung privater Accounts (z.B. private E-Mailadressen oder Social-Media-Konten) für die geschäftliche Kommunikation.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 11.                                  | Regelung der Art von Supportleistung, die der Arbeitgeber den Benutzern von Privatgeräten zur Verfügung stellt.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

<sup>80</sup> Sie sind durch Richtlinien der Informatikabteilung des Unternehmens hinsichtlich der technischen Umsetzung von BYOD zu ergänzen.

|     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12. | <p>Ergänzung zum Spesenreglement</p> <p>Festlegen der entschädigten Ausgaben des Arbeitnehmers im Zusammenhang mit BYOD:</p> <ul style="list-style-type: none"> <li>– (Anteil) Anschaffungskosten, (Anteil) Abonnementskosten, (Anteil) Amortisationskosten, Mobilfunkgebühren, Gebühren für Datenverbindung, Stromkosten, (Anteil) Lizenzkosten (z.B. für Anti-viren-, Textverarbeitungsprogramme), (Anteil) Reparaturkosten und (Anteil) Kosten eines Ersatzgerätes;</li> <li>– Allfällige Beteiligung an Garantieverlängerung, Erweiterung Supportdienstleistungen des Herstellers;</li> <li>– Allfällige Beteiligung an Prämien für Versicherungen gegen Verlust, Diebstahl oder Beschädigung des Gerätes;</li> <li>– Ausweisen von Kosten, welche zusätzlich zur arbeitsrechtlichen Entschädigungspflicht (Art. 327a Abs. 1 OR) ausbezahlt werden (zur Festsetzung des steuerpflichtigen Privatanteils).</li> </ul> |
| 13. | <p>Festlegen der Gründe für ein partielles oder vollständiges Sperren/Zurücksetzen des Gerätes:</p> <ul style="list-style-type: none"> <li>– «Jailbreak»/«Rooten» des Gerätes;</li> <li>– Auf dem Gerät wird Software installiert, welche für Sicherheitslücken bekannt ist, sofern diese nicht innert Frist durch den Arbeitnehmer deinstalliert wird;</li> <li>– Gerät geht verloren/wird gestohlen;</li> <li>– Überschreitung der maximalen Anzahl an Anmeldeversuchen.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 14. | <p>Gründe für den Rückzug der BYOD-Erlaubnis durch den Arbeitgeber:</p> <ul style="list-style-type: none"> <li>– Verwendung eines Gerätes/einer Softwareversion, welche durch die Software und den Support des Arbeitgebers nicht mehr unterstützt wird;</li> <li>– Verstoss gegen die BYOD-Guidelines oder andere IT-Nutzungsbestimmungen;</li> <li>– Verstoss gegen die Treuepflicht des Arbeitnehmers.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## V. Schlusswort

Der Nutzeffekt von Privatgeräten am Arbeitsplatz ist unbestritten. Gleichzeitig gilt es aber, die Sicherheit der betrieblichen IT-Assets und Informationsgüter sowie die Privatsphäre der Arbeitnehmer zu gewährleisten. Dazu werden immer öfter entsprechende Benutzer- und Nutzungsrichtlinien festgelegt. Sie sollen die Unternehmen technisch und juristisch absichern. Es gibt leider keine allgemeingültigen BYOD-Richtlinien für jede Art von Unternehmen. Es ist wichtig, dass die Geschäftsführung und IT eng mit HR, mit der Finanz- sowie der Rechtsabteilung eines Unternehmens zusammenarbeiten, um unternehmensweit geltende BYOD-Richtlinien festzulegen. Damit die Richtlinien verstanden und befolgt werden, sollte das Unternehmen darauf achten, klare und prägnante Formulierungen zu wählen.

In Branchen mit erhöhten Anforderungen an die Datensicherheit, wie z.B. bei Banken oder Spitälern, können Alternativen zu BYOD empfehlenswert sein.

Viele Arbeitgeber erreichen die gleichen Mobilitätsziele, wie sie mit BYOD erreicht werden sollen, indem sie ihren Mitarbeitern zwar das geschäftliche Gerät geben, diese aber auswählen lassen, welches Gerät sie möchten. Diesen Trend nennt man *Choose Your Own Device (CYOD)*<sup>81</sup>. Der Arbeitgeber legt dabei die Auswahl an verfügbaren Gerätemodellen fest und kauft sie ein. Aus dieser Angebotspalette kann sich dann der Arbeitnehmer für ein Gerät entscheiden und (im Rahmen der Vorgaben des Arbeitgebers) darauf einige persönliche Anwendungen installieren sowie das Gerät auch privat nutzen. Als Eigentümerin bestimmt das Unternehmen die Benutzungsbedingungen und die Kostenlimiten. Im Gegensatz zur geschäftlichen Nutzung privater Geräte wird bei

<sup>81</sup> Ebenso Reutter/Klaus (Fn. 13), S. 160; Miller (Fn. 7). Der EDÖB (Fn. 15) versteht hingegen unter CYOD etwas anderes: Die Arbeitnehmer kaufen ein «offiziell» unterstütztes Gerät (mit oder ohne Kostenbeteiligung des Arbeitgebers) und das Unternehmen bestimmt die Konfiguration des Gerätes. Änderungen der eingestellten Konfigurationen sind dann verboten.

CYOD also der Handlungsrahmen zur privaten Nutzung von geschäftlichen Geräten definiert<sup>82</sup>.

Als *Faustregel* gilt: Zuerst sollte man überlegen, ob ein BYOD für die spezifischen Verhältnisse geeignet

ist, oder ob nicht ein CYOD sinnvoller und sicherer ist. Wenn ein BYOD vereinbart oder toleriert wird, dann ist eine BYOD-Richtlinie zu empfehlen. Ansonsten können ungeplante Kosten- und Haftungsfolgen auf den Arbeitgeber zukommen.

<sup>82</sup> Der *EDÖB* (Fn. 15) spricht von Corporate Owned Personally Enabled (COPE). *Reutter/Klaus* (Fn. 13), S. 160, sprechen von Private Use Of Company Equipment (PUOCE).