Jusletter IT

Der mobile Arbeitnehmer

Autor: Urs Egli
Kategorie: Tagungsbericht
Region: Schweiz
Rechtsgebiete: Arbeitsrecht, Datenschutz, Datensicherheit
Zitiervorschlag: Urs Egli, Der mobile Arbeitnehmer, in: Jusletter IT Flash 28. Juni 2017

Die Digital Natives sind im Arbeitsleben angekommen. Ihre Smartphones sind ihr wichtigster Besitz. Sie sind Kommunikationsmittel, Portemonnaie, Shopping Center, Wissensdatenbank und Spielzeug in einem. Ihr Nutzungsverhalten ist Ausdruck ihrer Persönlichkeit und ohne ihre Smartphones sind sie verloren. Es ist selbstverständlich, dass Digital Natives ihre Smartphones auch für das Arbeiten einsetzen. Arbeitgeber müssen sich damit arrangieren. Sie sind gut beraten, dies aktiv und nicht aus einer Abwehrhaltung heraus zu tun. Sonst tragen sie nur die Risiken, ohne von den Chancen profitieren zu können.

Inhaltsverzeichnis

1. Das Wesen des Arbeitsvertrags

[Rz 1] Der Arbeitnehmer ist zur Leistung von Arbeit im Dienst des Arbeitgebers verpflichtet (Art. 319 Abs. 1 des Obligationenrechts [OR]). Er hat ihm seine Arbeitskraft zur Verfügung zu stellen. Ein bestimmter Erfolg ist nicht geschuldet.[1] Wie die Arbeitskraft eingesetzt wird, ist Sache des Arbeitgebers. Die vom Arbeitnehmer geschaffenen Arbeitsresultate gehören dem Arbeitgeber.[2]

[Rz 2]

Der Arbeitnehmer gliedert sich in die Betriebsorganisation ein und erbringt seine Arbeitsleistung nach den Weisungen des Arbeitgebers (Art. 319 und Art. 321d OR). Diese beziehen sich sowohl auf den Inhalt der Arbeitsleistungen als auch auf die Begleitumstände. Der Arbeitgeber hat ein Weisungsrecht.

[Rz 3] Im Gegenzug zahlt der Arbeitgeber dem Arbeitnehmer Lohn. Zudem hat er für sämtliche Unkosten aufzukommen, die dem Arbeitnehmer aus dem Arbeitsverhältnis erwachsen (Art. 327a OR). Er trägt das Unternehmerrisiko und darf dieses nicht auf den Arbeitnehmer abwälzen. [3]

[Rz 4] Das Arbeitsverhältnis ist von zwei Nebenpflichten geprägt, welche den Tausch «Zeit gegen Lohn» begleiten; der Fürsorgepflicht des Arbeitgebers (Art. 328 OR) und der Sorgfalts- und Treuepflicht des Arbeitnehmers (Art. 321a OR).

[Rz 5] Aus der Fürsorgepflicht des Arbeitgebers fliessen zahlreiche Pflichten, die dem Wohlergehen und dem Schutz des Arbeitnehmers dienen. Dazu gehört auch der Ferien- und Freizeitanspruch.

[Rz 6] Der Arbeitnehmer auf der anderen Seite hat seine Arbeit sorgfältig auszuführen und er hat Maschinen, Arbeitsgeräte, Anlagen und Fahrzeuge fachgerecht zu bedienen und sorgfältig zu behandeln (Art. 321a Abs. 1 und 2 OR). Er hat sich loyal zu verhalten und er hat alles zu unterlassen, was den Arbeitgeber wirtschaftlich schädigen könnte.

[Rz 7] Der Arbeitnehmer ist zudem zur Geheimhaltung verpflichtet (Art. 321a Abs. 4 OR). Unter die Geheimhaltungspflicht fallen nicht nur die Fabrikations- und Geschäftsgeheimnisse im engeren Sinn wie z.B. Pläne, Forschungsergebnisse, Preisinformationen, Kunden- und Lieferantenbeziehungen etc. Geheim zu halten sind vielmehr ganz generell sämtliche Informationen, welche der Arbeitgeber vertraulich behandelt haben will. [4]

[Rz 8] Die Geheimhaltungspflicht besteht nur für Informationen, die nicht bereits offenkundig sind und an denen der Arbeitgeber ein berechtigtes Geheimhaltungsinteresse hat. [5] Nicht der Geheimhaltung unterliegt sodann die Berufserfahrung des Arbeitnehmers. Als Berufserfahrung gelten diejenigen Kenntnisse, welche sich ein Arbeitnehmer während der Arbeit angeeignet hat. [6] Als eine einfache Regel zur Abgrenzung zwischen geschütztem Know-how im Eigentum des Arbeitgebers und der Berufserfahrung des Arbeitnehmers gilt: Alles, was der Arbeitnehmer im Kopf behalten kann, darf er auch nach Beendigung des Arbeitsvertrags weiter verwenden. Schriftlich dokumentiertes Know-how hingegen gehört dem Arbeitgeber und darf nicht mitgenommen werden. [7]

[Rz 9] Die Geheimhaltungspflicht kann vorsätzlich, aber auch fahrlässig verletzt werden. Sie ist auch verletzt, wenn Arbeitnehmer Geschäftsgeheimnisse für eigene Zwecke verwerten. Die vorsätzliche Verletzung des Fabrikations- und Geschäftsgeheimnisses ist zudem strafbar (Art. 162 des Strafgesetzbuches [StGB]).

[Rz 10] Der Arbeitnehmer haftet für den Schaden, den er dem Arbeitgeber absichtlich oder fahrlässig verursacht (Art. 321e Abs. 1 OR). Er haftet bei jedem Verschulden; also bei leichter, mittlerer und grober Fahrlässigkeit und natürlich bei Vorsatz. Bei leichter Fahrlässigkeit wird die Haftung jedoch regelmässig stark reduziert, denn Arbeitnehmer sind in Bezug auf die Haftung privilegiert. Der Grund dafür ist, dass das Betriebsrisiko nicht auf den Arbeitnehmer abgewälzt werden darf.

[Rz 11] Das Mass der vom Arbeitnehmer anzuwendenden Sorgfalt bestimmt sich nicht wie sonst üblich nur nach objektiven Kriterien. Vielmehr werden neben dem Berufsrisiko auch subjektive, in der Person des Arbeitnehmers liegende Kriterien wie sein Bildungsgrad und seine Fachkenntnisse und Fähigkeiten berücksichtigt; letztere jedoch nur, soweit der Arbeitgeber diese kennt oder hätte kennen müssen (Art. 321e Abs. 2 OR). Deshalb muss zum

Beispiel ein als unzuverlässig bekannter Arbeitnehmer besonders überwacht werden.[8] Wird ein Arbeitnehmer nicht genügend instruiert oder überwacht, reduziert sich seine Haftung.[9] Vor allem aber liegt die Verantwortung für die Auswahl eines Arbeitnehmers beim Arbeitgeber. Setzt er für eine bestimmte Arbeit einen ungeeigneten Arbeitnehmer ein, so muss er sich dies als Haftungsreduktion anrechnen lassen.[10]

[Rz 12] Zwar gibt es keine Höchstgrenze für Schadenersatzforderungen des Arbeitgebers. Einige kantonale Gerichte haben jedoch die Faustregel entwickelt, dass eine Schadenersatzforderung einen Monatslohn nicht übersteigen soll, wenn weder eine absichtliche noch eine grobfahrlässige Schädigung vorliegt.[11]

[Rz 13] All das gilt natürlich auch beim mobilen Arbeiten und die meisten sich dabei stellenden Fragen sind durch das geltende Arbeitsrecht und die Praxis aus der analogen Welt geklärt. Dies gilt insbesondere für den Kostenersatz und die Geheimhaltungspflicht. Es gilt aber auch für einen allfälligen Schadenersatzanspruch. Schädigt ein Arbeitnehmer seinen Arbeitgeber durch eine Pflichtverletzung beim mobilen Arbeiten, so kann der Arbeitgeber nicht mit einem substantiellen Schadenersatzanspruch rechnen, es sei denn, der Arbeitnehmer habe vorsätzlich gehandelt.

2. Auswirkungen des mobilen Arbeitens auf das Arbeitsverhältnis

[Rz 14] Mobiles Arbeiten hat wesentliche Auswirkungen auf den Kern des Arbeitsverhältnisses. Der wichtigste Unterschied zum standortgebundenen Arbeiten liegt in der grösseren Freiheit zur Gestaltung der Arbeit, die mit dem mobilen Arbeiten verbunden ist. Beim mobilen Arbeiten gliedern sich Arbeitnehmer aus der physischen Betriebsorganisation aus. Dadurch gewinnen sie Autonomie, respektive der Arbeitgeber verliert Kontrolle.

[Rz 15] Damit hängt auch ein zweiter Unterschied zusammen: Die Autonomie in Bezug auf die Einteilung der Arbeitszeit. Mobile Arbeitnehmer können ihre Arbeitszeit nicht nur freier bestimmen, sondern die Grenzen zwischen Arbeit und Freizeit sind bisweilen unscharf, etwa wenn E-Mails während der Freizeit abgerufen werden oder wenn die Arbeit im Home Office durch eine private Aktivität unterbrochen wird.

[Rz 16] Ein dritter Unterschied besteht darin, dass Arbeitnehmer in grossem Stil private Arbeitsgeräte für ihre berufliche Tätigkeit einsetzen. Das ist zwar nicht neu, hatte aber in der analogen Welt abgesehen von speziellen Berufen (Coiffeure, Metzger, Zimmerleute) keine wirkliche Bedeutung. Damit ist die Verwendung von Smartphones jedoch nicht vergleichbar, denn Smartphones prägen die Lebens- und Arbeitsweise der *Digital Natives*. Mit ihren Smartphones bringen die Digital Natives das Private ins Geschäftliche und umgekehrt.

[Rz 17] Das Arbeitsrecht geht davon aus, dass der Arbeitgeber die Arbeitsgeräte zur Verfügung stellt (Art. 327 Abs. 1 OR). Zwar sieht das Gesetz auch eine Regel vor für den Fall, dass Arbeitnehmer ihre eigenen Arbeitsgeräte verwenden. Dann ist dafür eine angemessene Entschädigung zu bezahlen, sofern nichts anderes verabredet oder üblich ist (Art. 327 Abs. 2 OR). Letzteres dürfte bei Smartphones der Fall sein, sofern diese nur für E-Mail- und Kalenderfunktionen verwendet werden.

[Rz 18] Der vierte wesentliche Unterschied schliesslich besteht darin, dass durch mobiles Arbeiten besondere Risikosituationen für die immateriellen Unternehmenswerte des Arbeitgebers geschaffen werden. Private IT-Geräte können ein Einfallstor für Cyber-Attacken sein, Gespräche im Zug können abgehört und Datenspeicher können verloren werden. Die Beispiele sind zahlreich und die Risiken nehmen laufend zu.

3. Organisationspflichten des Arbeitgebers im digitalen Umfeld

3.1. Records Management

[Rz 19] Records Management befasst sich mit der Dokumentation der unternehmerischen Tätigkeit.[12] Die Pflicht zur Dokumentation geht je nach Unternehmenszweck weiter oder weniger weit.

[Rz 20] An erster Stelle sind die Vorschriften des Obligationenrechts zur kaufmännischen Buchführung zu erwähnen (Art. 957–963b OR). Für die Geschäftsbücher und die Buchungsbelege besteht eine zehnjährige Aufbewahrungspflicht (Art. 958f Abs. 1 OR). Für die Geschäftskorrespondenz (Verträge, Briefe, E-Mails) lässt sich eine solche Aufbewahrungspflicht zwar nicht mehr direkt aus dem Rechnungslegungsrecht ableiten.[13] Sie ergibt sich jedoch aus zahlreichen weiteren Vorschriften, wie insbesondere aus dem Verantwortlichkeitsrecht (Art. 716a OR) sowie aus weiteren Aufbewahrungs- und Editionspflichten (z.B. aus der Editionspflicht des Beauftragten).[14]

[Rz 21] Aufbewahrungspflichten, die für alle Unternehmen gelten, erwachsen aus dem Steuerrecht und dem Sozialversicherungsrecht. Weitere Aufbewahrungspflichten sind unternehmensspezifisch, so etwa im Finanzwesen (Bankenaufsicht, Geldwäschereibekämpfung), im Industriesektor (Exportkontrolle, Produktesicherheit) und im Gesundheitswesen (Patientendossier und Heilmittelkontrolle).

[Rz 22] Besonders strenge Anforderungen müssen Geheimnisträger beachten, deren Geheimnis strafrechtlichen Schutz geniesst. Dies betrifft die Finanzindustrie[15], das Fernmeldewesen[16], das Gesundheitswesen[17] sowie die Anwälte und Notare[18]. Dies hat erhebliche Auswirkungen auf die Ausgestaltung der IT-Infrastruktur solcher Unternehmen. Für die Finanzindustrie hat die FINMA mit der Outsourcing Richtlinie und dem Anhang 3 zum Rundschreiben 2008/21 detaillierte Vorschriften zur IT erlassen. Und im Gesundheitswesen sowie generell in der öffentlichen Verwaltung besteht zurzeit aufgrund eines kontroversen Gutachtens von Prof. WOHLERS eine Unsicherheit, unter welchen Voraussetzungen Cloud Computing zulässig ist.[19]

[Rz 23] Im Bereich der öffentlichen Verwaltung besteht eine generelle Pflicht zur Aktenführung.[20] Sie ist das Gegenstück zum Akteneinsichtsrecht.[21] Letzteres hat seine Grundlage in der Bundesverfassung (Anspruch auf rechtliches Gehör).[22] Zudem verpflichtet auch das Öffentlichkeitsprinzip zur Aktenführung (Art. 6 Abs. 1 des Öffentlichkeitsgesetzes [BGÖ]) und schliesslich ist die Aktenführung je nach Verwaltungsorganisation sogar ausdrücklich gesetzlich geregelt (für den Bund in Art. 22 Abs. 1 der Regierungs- und Verwaltungsorganisationsverordnung [RVOV]).

[Rz 24] Behörden sind verpflichtet, den Nachweis der Verwaltungstätigkeit (Sachverhaltsabklärung und Entscheidungsgründe) jederzeit auf nachvollziehbare Weise zu gewährleisten. Die Behörde hat alles festzuhalten, was zur Sache gehört und wesentlich sein kann. Die Unterlagen sind von Beginn weg in chronologischer Reihenfolge abzulegen. Die systematische Aktenführung hat nach festgelegten, sachgerechten und zweckmässigen Kriterien zu erfolgen.[23]

[Rz 25] Diese Dokumentationspflicht trifft den Arbeitgeber. Ihr ist selbstverständlich auch beim mobilen Arbeiten nachzukommen. Der Arbeitgeber hat die erforderlichen Rahmenbedingungen zu schaffen und er kann (resp. muss) auch den Arbeitnehmer in die Einhaltung dieser Pflicht einbeziehen.

3.2. Datenschutz

[Rz 26] Der Datenschutz bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden (Art. 1 des Datenschutzgesetzes [DSG]). Das Datenschutzgesetz enthält Vorschriften, die bei der Bearbeitung von Personendaten zu beachten sind. Im vorliegenden Zusammenhang interessiert primär Art. 7 DSG betreffend Datensicherheit. Diese Bestimmung schreibt vor, dass Personendaten durch angemessene

technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Was angemessen ist, bestimmt sich nach der Art der bearbeiteten Daten, der Gefährdungslage und dem Stand der Technik (Art. 8 Abs. 2 der Verordnung zum Datenschutzgesetz [VDSG]).

[Rz 27] In den Anfängen der Informatik beschränkte sich der technische Schutz auf Massnahmen wie das Einrichten von Zugriffsbeschränkungen, Datenverschlüsselung, Protokollierung und dergleichen.[24] In den letzten Jahren hat sich die Bedrohungslage massiv verschärft. Die wichtigsten Themen sind heute (in der Reihenfolge der Aufzählung): Wiederherstellungs- und Notfallpläne nach Angriffen, Identity- und Accessmanagement, Mobile Device Security, Data Privacy, Security Governance und Management, Angriffs- und Penetration-Testing, Data Loss/Leakage Prevention, Security Incident und Eventmanagement, Einführung von NextGen-Security Lösungen, Konsolidierung der IT-Security-Infrastruktur, Schutz von Cloud-Lösungen, Compliance Monitoring und Implementierung von Standards.[25]

[Rz 28] Organisatorische Massnahmen sind z.B. Reglemente, Weisungen, Verträge, Schulungen und Kontrollen.[26]

[Rz 29] Die aus dem Datenschutz resultierenden Pflichten treffen den Datenbearbeiter.[27] Das ist der Arbeitgeber und nicht der Arbeitnehmer. Der Arbeitgeber kann diese Pflichten aber nur einhalten, wenn er auch und insbesondere die Arbeitnehmer einbezieht. Die grösste Gefährdung für die Informationssicherheit sitzt vor dem Bildschirm!

4. Erscheinungsformen des mobilen Arbeitens

4.1. Arbeiten im Home Office

[Rz 30] Jedermann verfügt heute über einen privaten Desktopcomputer oder über ein Notebook und viele Mitarbeitende setzen diese Geräte für ihre berufliche Tätigkeit ein. Dabei stellen sich vorab zwei Fragen:

- Auf welche Weise erfolgt der Datenaustausch mit der betrieblichen IT-Infrastruktur?
- Wie steht es um die Datensicherheit?

[Rz 31] Unternehmen sind gut beraten, die Infrastruktur für den Datenaustausch zur Verfügung zu stellen (z.B. VPN-Zugang, Remote Access auf den E-Mail-Dienst, Betrieb der Infrastruktur in der Cloud). Andernfalls behelfen sich die Arbeitnehmer selber, früher durch das Verschicken von Dateien auf private Mail-Accounts oder durch die Verwendung von Speichermedien, heute häufig über Cloud-Dienste.

[Rz 32] Die Datensicherheit ist bei privaten Geräten generell schlechter. Häufig haben mehrere Personen Zugang zu privaten Geräten und der Passwortschutz ist schlechter (mangels zwangsweise durchgesetzter Passwortwechsel). Der Virenschutz ist nicht sichergestellt und private WLAN-Netzwerke sind schlechter geschützt. Und schliesslich können Daten bei der Entsorgung privater Geräte in unbefugte Hände gelangen.

4.2. Arbeiten unterwegs

[Rz 33] Beim Arbeiten unterwegs kommen weitere Gefahrenquellen hinzu. Geräte können gestohlen werden oder verloren gehen und Datenverkehr über öffentliche oder ungesicherte Netze kann abgefangen werden. Eine grosse Gefahr für Geschäftsgeheimnisse stellt auch das Führen von Telefongesprächen in öffentlichen Verkehrsmitteln oder anderen öffentlichen Räumen dar. Ebenso können fremde Bildschirme leicht eingesehen werden.

4.3. Bring Your Own Device

[Rz 34] Unter dem Begriff BYOD (*Bring Your Own Device*) wird die Verwendung privater Endgeräte (Smartphones und Tablets) für geschäftliche Zwecke verstanden, wobei dies auf eine institutionalisierte Art mit Kenntnis und unter Mitwirkung des Arbeitgebers geschieht. Am häufigsten vorkommen dürfte die Verknüpfung privater Geräte mit dem geschäftlichen E-Mail und dem Kalender. Smartphones können aber auch zum Lesen und Schreiben von Texten verwendet werden. Daneben existieren besondere Apps für Geschäftsapplikationen (z.B. für die Zeiterfassung oder das Rapportwesen), welche die mobile Nutzung ermöglichen. Aber auch die übrigen Funktionen von Smartphones wie Kameras und Mikrofone können für geschäftliche Zwecke eingesetzt werden, z.B. für eine fotografische Dokumentation von Baumängeln oder die Aufnahme von Maschinengeräuschen bei Wartungsarbeiten. Und schliesslich ist zu erwähnen, dass die wichtigste Nutzungsform von Smartphones (die Nutzung sozialer Medien und der Zugang zu Informationen) auch geschäftlichen Zwecken dienen kann.

[Rz 35] Ein wichtiger Aspekt bei BYOD ist der technische Schutz von mobilen Endgeräten. Anzumerken ist dazu, dass Smartphones generell weniger gut geschützt werden können als Notebooks. Wie der technische Schutz umgesetzt wird, ist eine technische Frage.

[Rz 36] Aus juristischer Sicht interessieren im Zusammenhang mit BYOD vorwiegend die folgenden Themen: [28]

- Haben Arbeitnehmer einen Anspruch, das eigene Smartphone für das Arbeiten verwenden zu dürfen? Antwort: Nein.
- Können Arbeitnehmer verpflichtet werden, ihr eigenes Smartphone für das Arbeiten zu verwenden? Antwort: Nein.
- Hat ein Arbeitnehmer Anspruch auf Spesenersatz für die Verwendung eines privaten Geräts? Antwort: Ja, aber das kann vertraglich wegbedungen werden, auch konkludent, was in der Regel der Fall ist. Die Wegbedingung gilt aber nicht für die Verbindungskosten.
- Wer trägt die Verantwortung für die IT-Security? Antwort: Der Arbeitgeber, wobei der Arbeitnehmer eine Mitverantwortung trägt.
- Wie steht es um die Persönlichkeitsrechte der Arbeitnehmer, wenn Arbeitgeber wegen Massnahmen der IT-Security (Wiping) und zu Kontrollzwecken auf private Daten zugreifen, die auf den mobilen Endgeräten gespeichert sind? Antwort: Das ist zulässig, aber nur mit Zustimmung des Arbeitnehmers.
- Sind private Geräte ausreichend lizenziert für den betrieblichen Einsatz? Antwort: Wohl eher nicht.

4.4. Nutzung von Cloud-Diensten

[Rz 37] Unternehmen lagern ihre Informatik immer öfter in die Cloud aus. Eines der Motive dafür ist, das mobile Arbeiten zu erleichtern. Professionelle Cloud-Dienste haben in der Regel einen hohen technischen Sicherheitsstandard. Dem Arbeitgeber bleibt die Pflicht, seine Arbeitnehmer mittels organisatorischer Massnahmen in die Einhaltung der Sicherheitsstandards einzubeziehen.

[Rz 38] Wenn Arbeitnehmer private Cloud-Dienste verwenden (z.B. Dropbox oder Evernote), so ist das problematisch. Solche Dienste haben einen tieferen Sicherheitsstandard. Insbesondere bei den kostenlosen Einsteigerabonnements besteht keinerlei Gewähr für die Informationssicherheit. Es ist vielmehr zu befürchten, dass solche Anbieter Daten für eigene Zwecke auswerten. Zudem werden die Daten durch die automatische Synchronisation aller am Cloud-Dienst angeschlossenen Endgeräte verbreitet. Und schliesslich hat nur der Arbeitnehmer direkten Zugriff auf die mit privaten Cloud-Diensten verarbeiteten Daten. Damit verliert der Arbeitgeber jegliche Kontrolle über die Daten. Arbeitgeber sollten deshalb die Verwendung privater Cloud-Dienste zur Verwaltung betrieblicher Daten untersagen.

5. Arbeitszeitkontrolle

[Rz 39] Das Arbeitsgesetz (ArG) enthält Vorschriften zur wöchentlichen Höchstarbeitszeit (Art. 9 ArG), zur Ruhezeit (Art. 15 und 15a ArG), zur Nacht- und Sonntagsarbeit (Art. 16 und 18 ArG) und zur Überzeit (Art. 12 ArG). Dies bedingt eine Erfassung der Arbeitszeit, welche deshalb vom Arbeitsgesetz ebenfalls vorgeschrieben wird (Art. 46 ArG und Art. 73 ff. der Verordnung 1 zum Arbeitsgesetz [ArGV 1]).

[Rz 40] Die (ordentliche) Zeiterfassung sieht die Erfassung der Arbeitszeit mit Lage und Pausen vor (Art. 73 Abs. 1 ArGV 1). Bei der vereinfachten Zeiterfassung hingegen ist nur die tägliche Gesamtdauer zu erfassen (Art. 73b Abs. 1 ArGV 1). Die vereinfachte Zeiterfassung ist nur zulässig, wenn die Arbeitnehmer eine namhafte Zeitautonomie haben (Art. 73b Abs. 1 ArGV 1). Die vereinfachte Zeiterfassung ist entweder in einer kollektiven Betriebsvereinbarung zu regeln oder in kleinen Unternehmen (weniger als 50 Arbeitnehmende) im Arbeitsvertrag (Art. 73b Abs. 1 und 3 ArGV 1). Der Verzicht auf eine Zeiterfassung ist nur bei Jahreseinkommen über CHF 120’000 möglich, wenn gleichzeitig grosse Zeitautonomie besteht und ein GAV existiert (Art. 73a Abs. 1 ArGV 1).

[Rz 41] Die Aufzeichnung der Arbeitszeit ist mit verschiedenen technischen Mitteln möglich (Stempeluhr, Zutrittsbadge, Login). Sie kann auch ganz dem Arbeitnehmer übertragen werden (Rapportbuch, Excel). Schliesslich wird der Pflicht zur Erfassung der Arbeitszeit auch durch die Einrichtung fester Arbeitszeiten nachgekommen. [29]

[Rz 42] Beim mobilen Arbeiten stellt sich die Frage, was als Arbeitszeit gilt und was nicht. Arbeitgebern ist zu empfehlen, diesbezüglich Klarheit zu schaffen.

[Rz 43] Klar ist, dass Reisezeit (exkl. der Arbeitsweg) als Arbeitszeit gilt, unabhängig davon, ob während der Reise noch zusätzliche Arbeit erledigt wird. [30] Das kann bei sehr langen Reisezeiten (Geschäftsreisen, Flüge) zu unbilligen Ergebnissen führen. Für solche Fälle sollte in einem Reglement die maximal anrechenbare Höchstarbeitszeit festgelegt werden, was zulässig ist. [31]

[Rz 44] Fraglich ist, ob das permanente Abrufen des Mail-Accounts (auch in der Freizeit) als Arbeitszeit gilt. [32] Zwar könnte man dies als Ausgleich für den umgekehrten Fall sehen, nämlich die permanente Aufrechterhaltung privater sozialer Kontakte während der Arbeitszeit. Es ist jedoch anzunehmen, dass Gerichte (z.B. im Zusammenhang mit einer Überstundenforderung) das Abrufen von E-Mails als Arbeitszeit beurteilen würden. Arbeitgeber sollten deshalb in Erwägung ziehen, das Abrufen des Mail-Accounts ausserhalb der Arbeitszeit zu untersagen, wenn sie sich diesem Risiko nicht aussetzen wollen.

[Rz 45] Weitere Grenzfälle sind die persönliche Weiterbildung durch Lektüre von Zeitschriften ausserhalb der Arbeitszeit, Aktivitäten (z.B. Referate), die der eigenen Profilierung dienen, sowie die Wahrnehmung sozialer Kontakte mit geschäftlichem Hintergrund.

[Rz 46] Problematisch ist schliesslich auch die Einhaltung der Ruhezeit und des Nacht- und Sonntagsarbeitsverbots. Ein Arbeitgeber dürfte deshalb gemäss geltendem Recht nicht tolerieren, dass Arbeitnehmer zu Hause während der Nacht oder am Sonntag arbeiten.

[Rz 47] Die gesetzlichen Bestimmungen zur Arbeitszeit sind nicht für das mobile Arbeiten geschaffen worden. Ihre Anwendung auf das mobile Arbeiten führt zu unbefriedigenden Ergebnissen. Das gilt jedenfalls für Arbeitnehmer, die über eine gewisse Zeit- und Gestaltungsautonomie verfügen.

6. Eigenverantwortung des Arbeitnehmers

[Rz 48]

Der Arbeitgeber muss dem Arbeitnehmer nicht in jedem Detail vorschreiben, was er zu tun hat. Der Arbeitnehmer hat eine Sorgfaltspflicht und damit auch eine Eigenverantwortung. Das gilt auch für das Arbeiten im digitalen Raum. Das Mass der anzuwendenden Sorgfalt bestimmt sich nach subjektiven Kriterien wie dem Bildungsgrad, den Fachkenntnissen und den Fähigkeiten des Arbeitnehmers, soweit der Arbeitgeber diese kennt oder hätte kennen müssen (siehe Ziffer 1). Bei *Digital Natives* dürfen dabei höhere Anforderungen an die Eigenverantwortung gestellt werden. Das Gleiche gilt für Führungspersonen und F&E-Mitarbeiter im Hinblick auf die Wahrung von Geschäftsgeheimnissen, für Berufsgeheimnisträger (z.B. medizinisches Personal) im Hinblick auf die Wahrung desselben sowie für Beamte im Zusammenhang mit dem Amtsgeheimnis.

[Rz 49] Konkret bedeutet es, dass man heute von Arbeitnehmern in Büroberufen erwarten darf, dass sie die wichtigsten Regeln betreffend den Umgang mit Zugangsdaten und Passwörtern kennen. Ebenso darf man von Arbeitnehmern mit Reisetätigkeit erwarten, dass sie beim Arbeiten in öffentlichen Räumen und in öffentlichen Verkehrsmitteln die elementaren Sorgfaltsregeln beachten.

[Rz 50] Auch was die Dokumentationspflicht betrifft, darf man von Arbeitnehmern Vorkenntnisse erwarten, z.B. bei HR-Angestellten Kenntnisse zum Personaldossier und bei Medizinalpersonal Kenntnisse zum Patientendossier. Beamte schliesslich sollten die Grundprinzipien des Aktenwesens kennen.

[Rz 51] Die Oberverantwortung für das Records Management liegt jedoch beim Arbeitgeber. Die Erstellung eines Konzepts für das Records Management sowie die Bereitstellung der technischen Mittel sind seine Aufgaben. Ein Arbeitnehmer kann sich aber auch hier nicht von jeglicher (Mit-)Verantwortung verabschieden. Ein Berufsgeheimnisträger, der erkennt, dass sein Arbeitgeber über ein ungenügendes Records Management verfügt, muss diesen darauf hinweisen und selber aktiv werden. HR-Angestellte müssen selber in der Lage sein, eine Triage der Dokumente zu machen, welche ins Personaldossier gehören.

7. Überwachung

[Rz 52] Beim mobilen Arbeiten erlangen Überwachungsmassnahmen eine grössere Bedeutung, da die gewissermassen «natürliche» Überwachung, die mit der Anwesenheit am Betriebsstandort verbunden ist, entfällt.

[Rz 53] Die systematische Leistungskontrolle ist durch eine Verordnung zum Arbeitsgesetz untersagt (Art. 26 der Verordnung 3 zum Arbeitsgesetz [ArGV 3]). Hinzunehmen ist jedoch die Überwachung der Arbeitnehmer, wenn andere zulässige Überwachungsgründe vorliegen (z.B. Unfallverhütung, Schutz von Personen und Sachen, Überwachung der IT-Infrastruktur, Sicherstellung der Einhaltung von Weisungen).[33] Auch zur Leistungskontrolle ist eine Überwachung zulässig, sofern sie nicht systematisch erfolgt.[34] Die personenbezogene Überwachung ist nur in Verdachtsfällen oder stichprobenweise zulässig. Zudem sind vor einer Überwachung weniger einschneidende Massnahmen (z.B. technische Schutzmassnahmen) zu ergreifen.[35]

[Rz 54] In folgenden zwei Fällen hat das Bundesgericht die Zulässigkeit von Überwachungsmassnahmen exemplarisch geprüft. In BGE 139 II 7 wurde die Überwachung eines Arbeitnehmers mittels einer auf dem Arbeitsplatzcomputer installierten Spionagesoftware für unzulässig erklärt, obwohl dadurch eine eklatante Verletzung des Arbeitsvertrages zutage gefördert wurde. Die Massnahme war nicht verhältnismässig. In BGE 130 II 425 ging es um die Verhältnismässigkeit einer Installation von GPS-Überwachungsgeräten in Geschäftsfahrzeugen von Aussendienstmitarbeitern. Die Vorinstanzen taxierten dies noch als unzulässige Überwachungsmassnahme. Das Bundesgericht differenzierte zwischen einer (unzulässigen) GPS-Überwachung in Echtzeit und einer (zulässigen) GPS-Überwachung, die lediglich im Nachhinein erfolgte, indem das Überwachungssystem tägliche Aufstellungen über die angefahrenen Orte erstellte.

[Rz 55] Zu beachten sind die strafrechtlichen Schranken der Überwachung. Persönlich adressierte Briefe (nicht aber E-Mails) sind durch das Schriftgeheimnis (Art. 179 StGB), Telefongespräche durch das Abhör- und Aufnahmeverbot (Art. 179 bis StGB) und besonders schützenswerte Personendaten und Persönlichkeitsprofile durch Art. 179 novies StGB geschützt.

8. Reglemente

[Rz 56] Allgemeine Anstellungsbedingungen (Personalreglemente, Personalhandbücher, Allgemeine Arbeitsbedingungen oder Allgemeine Mitarbeiterbedingungen) werden vom Arbeitgeber verfasst und enthalten in der Regel eine umfassende Darstellung der Rechte und Pflichten betreffend das Arbeitsverhältnis. Allgemeine Anstellungsbedingungen sind Bestandteil des Arbeitsvertrags, wenn auf sie in einem Einzelarbeitsvertrag verwiesen wird.[36] Sie können deshalb nicht einseitig geändert werden.[37] Möglich ist jedoch die stillschweigende Änderung durch widerspruchslose Entgegennahme und Anwendung.[38]

[Rz 57] Weisungen demgegenüber sind Anordnungen, die der Arbeitgeber einseitig gestützt auf sein Weisungsrecht (Art. 321d OR) erlässt.[39] Das Weisungsrecht umfasst insbesondere auch das Recht des Arbeitgebers, dem Arbeitnehmer die zu erledigende Arbeit zuzuteilen und ihm Anweisungen zu geben, wie die Arbeiten auszuführen sind. Dabei muss er sich am Inhalt des Arbeitsvertrags orientieren und die Persönlichkeitsrechte des Arbeitnehmers wahren.[40] Zudem darf das Weisungsrecht die wesentlichen Kriterien des Tausches «Zeit gegen Lohn» nicht ändern (finanzielle Ansprüche, Berechnung der Arbeitszeit).[41]

[Rz 58] Der Arbeitnehmer hat solche Weisungen zu befolgen (Art. 321d Abs. 2 OR).

[Rz 59] Weisungen können entweder in der Form allgemeiner Anordnungen (z.B. Haus- oder Betriebsordnung) oder als individuell an einzelne Arbeitnehmer gerichtete Anweisungen ergehen.[42] Weisungen sind empfangs-, aber nicht zustimmungsbedürftig.[43] Sie müssen somit dem Arbeitnehmer lediglich zur Kenntnis gebracht werden.[44] Sein Einverständnis braucht es nicht. Weisungen können deshalb im Unterschied zum Arbeitsvertrag durch den Arbeitgeber einseitig geändert werden.

[Rz 60] Die Vorschriften für das digitale und mobile Arbeiten sollten so weit als möglich in der Form von Weisungen und nicht in der Form zustimmungsbedürftiger Allgemeiner Arbeitsbedingungen erlassen werden. Erstens ist es Sache des Arbeitgebers, Vorschriften zum Geheimnisschutz, zur Informationssicherheit und zum Records Management zu erlassen. Zweitens betreffen solche Anordnungen nicht den Kern des Arbeitsverhältnisses und drittens müssen diese Regeln wegen der schnellen technischen Entwicklung häufig angepasst werden. Zur Regelung von Entschädigungsfragen ist eine solche Weisung indessen nicht geeignet. Dieser Themenbereich sollte im Spesenreglement behandelt werden.

[Rz 61] Aufgrund der dynamischen Entwicklung dieser Themen ist ein iteratives Vorgehen sinnvoll. Möglicherweise bringen thematische Einzelanweisungen (z.B. zum Passwortschutz) mehr als umfassende Reglemente. Bei solchen besteht die Gefahr, dass sie schon beim Erlass veraltet sind oder gar nicht zur Kenntnis genommen werden.

[Rz 62] Es ist darauf zu achten, dass Weisungen vom zuständigen betrieblichen Organ erlassen werden und dass dies dokumentiert wird (GL-Protokoll, VR-Protokoll). Und schliesslich sind die Weisungen und Reglemente durchzusetzen. Dies setzt voraus, dass die Arbeitnehmer in geeigneter Form informiert und geschult werden und dass die Einhaltung überwacht wird.

[Rz 63] Typische Inhalte solcher IT-Reglemente sind:[45]

- Vorschriften zur sorgfältigen Benutzung der betrieblichen IT-Mittel
- Sicherung gegen Diebstahl und Verlust
- Umgang mit Zugangsdaten und Passwörtern
- Vorschriften zum Umgang mit betrieblichen Daten
- Private Nutzung der betrieblichen IT-Mittel
- Umgang mit E-Mails
- Benutzung der betrieblichen Telekommunikationsanschlüsse
- Formen unzulässiger Nutzung
- Nutzung sozialer Medien
- Überwachung
- Sanktionen

[Rz 64] Bei BYOD sind zusätzlich folgende Themen zu regeln: [46]

- Beidseitige Freiwilligkeit der Nutzung von BYOD
- Kostentragung
- Zustimmung des Arbeitnehmers zur Speicherung betrieblicher Daten auf seinem Gerät
- Verpflichtung zur Einrichtung einer PIN für die Entsperrung des Bildschirms (was technisch erzwungen werden kann)
- Verpflichtung zur Durchführung von Betriebssystem-Updates (was technisch erzwungen werden kann)
- Mobile Device Management (lesen, ändern und löschen von auf mobilen Geräten gespeicherten Daten durch den Arbeitgeber)
- Einsatz spezieller Sicherheitstools (z.B. Verpflichtung zur Verwendung von E-Mail-Verschlüsselung)
- Benachrichtigungspflicht bei Verlust des mobilen Geräts
- Einstellungen der Gerätekonfiguration und Verbot zur Nutzung bestimmter Software
- Verbot der Umgehung von Sicherheitsmechanismen

9. Fazit

[Rz 65] Mobiles Arbeiten hat das Potential, einen Paradigmenwechsel im Arbeitsrecht zu bewirken. Arbeitnehmer können beim mobilen Arbeiten über die Arbeitszeit und damit über ein wesentliches Element des Arbeitsverhältnisses selber bestimmen. Sie haben eine grössere Autonomie; nicht nur in Bezug auf die Arbeitszeit, sondern ganz generell bei der Gestaltung ihrer Arbeit. Dem sollte auch die Jurisprudenz Rechnung tragen und es stellt sich die Frage, ob nicht der Tausch «Zeit gegen Lohn» etwas in den Hintergrund treten sollte zugunsten einer beschränkten Ergebnisverantwortung. Im geltenden Arbeitsrecht fehlen geeignete Lösungsansätze für moderne Arbeitsformen. Vielmehr werden alle Arbeitsverhältnisse über einen Leist geschlagen. Dies zeigt die laufende Diskussion zur Arbeitszeitkontrolle.

[Rz 66] Arbeitgeber, die ihren Arbeitnehmern das mobile Arbeiten erlauben, sollten primär die folgenden drei Themen angehen:

- Ist sichergestellt, dass die beim mobilen Arbeiten generierten Daten in das betriebliche Records Management System Eingang finden?
- Werden die betrieblichen Vorschriften zur Informationssicherheit durchgesetzt?
- Wie wird mit der Erfassung der Arbeitszeit umgegangen?

[Rz 67] Arbeitnehmer sollten bei diesen Themen stärker in die Verantwortung genommen werden. *Digital Natives* können besser mit den Risiken des digitalen Lebens umgehen als viele ihrer Vorgesetzten, die sich in der digitalen Welt als «Einwanderer» zu Recht finden müssen. Die *Digital Natives* sollen diese Erfahrung auch in das Arbeitsleben

einbringen. Das führt zu mehr Freiheit bei der Gestaltung des Arbeitsumfelds, aber auch zu mehr Verantwortung in der Form gesteigerter Sorgfaltspflichten.

Dr. URS EGLI, Rechtsanwalt, Zürich.

---

1 WOLFGANG PORTMANN/ROGER RUDOLPH, in: Heinrich Honsell/Nedim Peter Vogt/Wolfgang Wiegand (Hrsg.), Basler Kommentar Obligationenrecht I, 6. Auflage, Basel 2015, Art. 319 OR N 7; ULLIN STREIFF/ADRIAN VON KAENEL/ROGER RUDOLPH, Praxiskommentar zum Arbeitsvertrag, 7. Auflage, Zürich 2012, Art. 319 OR N 2 und 4.

2 WOLFGANG PORTMANN/JEAN-FRITZ STÖCKLI, Schweizerisches Arbeitsrecht, 3. Auflage, Zürich/St. Gallen 2013, RZ 589; ADRIAN STAEHELIN, Zürcher Kommentar, Obligationenrecht, Teilband V 2c, Der Arbeitsvertrag, 4. Auflage, Zürich/Basel/Genf 2006, Art. 321b OR N 8; STREIFF/VON KAENEL/RUDOLPH (Fn. 1), Art. 321b OR N 5, resp. für immaterielle Güter Art. 332 OR sowie STREIFF/VON KAENEL/RUDOLPH (Fn. 1), Art. 332 OR N 2 ff.

3 STREIFF/VON KAENEL/RUDOLPH (Fn. 1), Art. 322a OR N 2.

4 PORTMANN/RUDOLPH (Fn. 1), Art. 321a OR N 24 f.; STREIFF/VON KAENEL/RUDOLPH (Fn. 1), Art. 321a OR N 12.

5 STAEHELIN (Fn. 2), Art. 321a OR N 44; STREIFF/VON KAENEL/RUDOLPH (Fn. 1) Art. 321a OR N 12.

6 URS WICKIHALDER, Die Geheimhaltungspflicht des Arbeitnehmers, Diss. Bern 2004, 37.

7 Zur Interessenabwägung bei der Abgrenzung der Berufserfahrung gegenüber Geschäftsgeheimnissen siehe URS EGLI, Softwareentwicklung im Arbeitsverhältnis, ArbR 2007, 29 f.

8 AGer Solothurn-Lebern in JAR 1993 S. 130, OGer AR in JAR 1994 S. 135, KGer SG in JAR 1988, S. 308 und CA GE in JAR 1987 S. 167.

9 STAEHELIN (Fn. 2), Art. 321e OR N 30; STREIFF/VON KAENEL/RUDOLPH (Fn. 1), Art. 321e OR N 3.

10 PORTMANN/RUDOLPH (Fn. 1), Art. 321e OR N 8; STAEHELIN (Fn. 2), Art. 321e OR N 29; STREIFF/VON KAENEL/RUDOLPH (Fn. 1), Art. 321e OR N 3.

11 STAEHELIN (Fn. 2), Art. 321e OR N 27; siehe dazu auch STREIFF/VON KAENEL/RUDOLPH (Fn. 1), Art. 321e OR N 12 mit Verweisen.

12 JACQUES BEGLINGER/DANIEL BURGWINKEL/BEAT LEHMANN/PETER K. NEUENSCHWANDER/BRUNO WILDHABER, Records Management, 2. Auflage, Zürich 2008, 37.

13 Die Geschäftskorrespondenz ist seit der Revision der Buchführungs- und Rechnungslegungsvorschriften des Obligationenrechts (in Kraft seit 1. Januar 2013) nicht mehr bei den aufzubewahrenden Belegen erwähnt (siehe auch BRUNO WILDHABER, Information Governance, Zürich 2015, 94).

14 WILDHABER (Fn. 13), 105 ff.

15 Bankgeheimnis (Art. 47 des Bankengesetzes [BankG]).

16 Fernmeldegeheimnis (Art. 43 des Fernmeldegesetzes [FMG]).

17 Ärztliches Berufsgeheimnis (Art. 321 StGB).

18 Berufsgeheimnis der Anwälte und Notare (Art. 321 StGB).

19 WOLFGANG WOHLERS, Auslagerung einer Datenbearbeitung und Berufsgeheimnis (Art. 321 StGB), in: digma 2016.

20 ULRICH HÄFELIN/GEORG MÜLLER/FELIX UHLMANN, Allgemeines Verwaltungsrecht, 7. Auflage, RZ 1552 ff.

21 GEROLD STEINMANN, in: Bernhard Ehrenzeller/Benjamin Schindler/Rainer J. Schweizer/Klaus A. Vallender (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, Art. 29 BV N 55.

22 GIOVANNI BIAGGINI, in: Ehrenzeller/Schindler/Schweizer/Vallender (Fn. 21), Art. 29 BV N 21.

23 Urteil des Bundesgerichts 8C_319/2010 vom 15. Dezember 2010, E. 2.2.1.

24 Eine Auflistung der technischen Schutzmassnahmen findet sich bei DAVID ROSENTHAL/YVONNE JÖHRI, Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 7 Abs. 1 DSG N 8.

25 Computerworld Swiss IT 2017.

26 Weiterführend siehe ROSENTHAL/JÖHRI (Fn. 24), Art. 7 Abs. 1 DSG N 9.

27 ROSENTHAL/JÖHRI (Fn. 24), Art. 3 Bst. i DSG N 105.

28 MARIAN ARNING/FLEMMING MOOS/MAXIMILIAN BECKER, Vertragliche Absicherung von Bring Your Own Device, Was in einer Nutzungsvereinbarung zu BYOD mindestens enthalten sein sollte, CR 2012, S. 592–598; NICOLE BERANEK ZANON, Bring your own device (BYOD) aus rechtlicher Sicht, in: Jusletter IT 12. September 2012; NICOLAS BIRKHÄUSER/MARCEL HADORN, BYOD – Bring Your Own Device, SJZ 109/2013, S. 201; SÉBASTIEN FANTI, Bref aperçu des aspects légaux du BYOD (Bring Your Own Device), in: Dunand Jean-Philippe/Mahon Pascal (Hrsg.), Internet au travail, Volume 5, Zürich 2014, S. 165–203; ROLAND PORTMANN, Private Smartphones im Geschäftsumfeld, digma 2012, S. 42; MARK. A. REUTTER/SAMUEL KLAUS, Rechtliche Stolpersteine bei «BYOD», digma 2012, S. 160; MICHÈLE STUTZ/NOEMI VALLONI, Social Media und Recht für Unternehmen, Zürich/Basel/Genf 2015; ISABELLE WILDHABER/SILVIO HÄNSENBERGER, 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, ARV/DTA 2016, S. 151–165; ISABELLE WILDHABER/SILVIO HÄNSENBERGER, Internet am Arbeitsplatz, ZBJV 152/2016, S. 307.

29 Modalitäten der Arbeitszeiterfassung – Ergänzung zur Weisung des SECO in Sachen Arbeitszeiterfassung vom 4. Juli 2014.

30 PORTMANN/RUDOLPH (Fn. 1), Art. 321 OR N 8; STREIFF/VON KAENEL/RUDOLPH (Fn. 1), Art. 321 OR, N 9.

31 STREIFF/VON KAENEL/RUDOLPH (Fn. 1), Art. 321 OR, N 9.

32 ADRIAN VON KAENEL, Die ständige Erreichbarkeit des Arbeitnehmers, ARV 2009, 9 f. (bejahend mit einer ausführlichen arbeitsrechtlichen Analyse).

33 BGE 130 II 425 (Pra 94 (2005) Nr. 71), E. 4.4.

34 BGE 130 II 425 (Pra 94 (2005) Nr. 71), E. 4.2.

35 BGE 139 II 7 (Pra 102 (2013) Nr. 82), E. 5.5.4.

36 PORTMANN/RUDOLPH (Fn. 1), Art. 320 OR N 18; PORTMANN/STÖCKLI (Fn. 2), RZ 95; STREIFF/VON KAENEL/RUDOLPH (Fn. 1), Art. 320 OR N 2.

37 STREIFF/VON KAENEL/RUDOLPH (Fn. 1), Art. 320 N 3, für welche eine Klausel, die solches vorsieht, der Ungewöhnlichkeitsregel unterliegt.

38 STREIFF/VON KAENEL/RUDOLPH (Fn. 1), Art. 320 OR N 3.

39 PORTMANN/STÖCKLI (Fn. 2), RZ 561; STREIFF/VON KAENEL/RUDOLPH (Fn. 1), Art. 321d OR N 2.

40 STAEHELIN (Fn. 2), Art. 321d OR N 18; PORTMANN/STÖCKLI (Fn. 2), RZ 576; STREIFF/VON KAENEL/RUDOLPH (Fn. 1), Art. 321d OR N 3.

41 STREIFF/VON KAENEL/RUDOLPH (Fn. 1), Art. 321d OR N 3.

42 STREIFF/VON KAENEL/RUDOLPH (Fn. 1), Art. 321d OR N 5.

43 PORTMANN/RUDOLPH (Fn. 1), Art. 321d OR N 2; STREIFF/VON KAENEL/RUDOLPH (Fn. 1), Art. 321d OR N 2.

44 STREIFF/VON KAENEL/RUDOLPH (Fn. 1), Art. 321d OR N 2.

45 WILDHABER/HÄNSENBERGER, Internet am Arbeitsplatz (Fn. 28), 337 ff.

46 ARNING/MOOS/BECKER (Fn. 28).