



Mobile Device Management – rechtliche Fragen

Smartphones und Tablet-PCs haben entscheidend zur mobilen Vernetzung im Berufs- und Privatleben beigetragen. Es ist selbstverständlich, überall und jederzeit mit dem Internet verbunden zu sein. Verbunden sein heißt auch, Zugriff auf Kommunikationsinfrastrukturen und Anwendungen zu haben, im privaten Bereich etwa auf soziale Netzwerke, im beruflichen Bereich auf Personal Information Manager wie Outlook, Lotus Notes oder ERP- und CRM-Systeme.

Von Thorsten Walter und Joachim Dorschel

Dabei verschwimmen die Grenzen zwischen beruflicher und privater Sphäre. Mitarbeiter bringen private Geräte ins Unternehmen mit. Arbeitgeber stellen ihren Arbeitnehmern mobile Geräte zur Verfügung, welche diese auch privat nutzen.

Erscheinungsformen

Juristisch wird in diesem Zusammenhang seit Längerem das Phänomen des „Bring Your Own Device“ diskutiert. Der rechtlich relevante Sachverhalt ist aber weitreichender:

- Private Geräte werden für berufliche Zwecke und unternehmenseigene Geräte für private Zwecke genutzt, dies jeweils mit oder ohne Zustimmung des Arbeitgebers.
 - Private Geräte ersetzen unternehmenseigene Arbeitsmittel, was mit einem finanziellen Ausgleich für den Arbeitnehmer verbunden ist.
- Die Einflussmöglichkeiten des Arbeitgebers auf Art und Umfang der Verwendung stehen dabei in unmittelbarem Zusammenhang mit den Eigentumsverhältnissen an den verwendeten Geräten. Über Geräte, die in seinem Eigentum stehen und die ausschließlich zur dienstlichen Nutzung überlassen werden, kann der Arbeitgeber frei

disponieren. Er kann das Gerät jederzeit gegen ein anderes – auch geringwertigeres – Gerät tauschen oder das Gerät ganz einziehen. Überlässt der Arbeitgeber das Gerät auch zur privaten Nutzung, sind seine Einflussmöglichkeiten eingeschränkt. Dies gilt noch mehr, wenn das eingesetzte Gerät im Eigentum des Arbeitnehmers steht.

Regelungsmöglichkeiten des Arbeitgebers

Es ist wenig überraschend, dass die Nutzung privater IT-Geräte im Unternehmen ohne Zustimmung des Arbeitgebers unzulässig ist. Tatsächlich ist genau dies aber der Regelfall: Mitarbeiter, die nur einen Desktop-PC haben, nutzen ihren privaten Laptop für Dienstreisen. Daten werden auf private USB-Sticks kopiert, der Outlook-Kalender mit dem Smartphone synchronisiert.

» Stellt der Arbeitgeber das Gerät für die dienstliche Nutzung, kann er im Rahmen des Direktionsrechts auch die Art der Nutzung vorschreiben. «

Duldet ein Arbeitgeber einen solchen Wildwuchs, wird er rechtlich so behandelt, als habe er die Nutzung der privaten Geräte im Unternehmen vorbehaltlos und ohne jede Einschränkung erlaubt. Damit hat er sich seiner Einfluss- oder Kontrollmöglichkeit weitgehend begeben. Eine spätere Änderung dieses Zustandes ist sowohl technisch als auch juristisch schwierig.

Um Schwierigkeiten von vornherein aus dem Weg zu gehen, sollte der Arbeitgeber den zulässigen Umgang mit mobilen Geräten schon vor ihrer Nutzung im Unternehmen regeln.

1. Direktionsrecht

Vorbehaltlich einer anderen Regelung im Arbeitsvertrag oder in einer Vereinbarung mit dem Betriebsrat (Betriebsvereinbarung) hat der Arbeitgeber ein Direktionsrecht über die Umstände der vertraglich geschuldeten Arbeitsleistung. Dies gilt auch für die Entscheidung darüber, mit welchen technischen Mitteln der Arbeitnehmer arbeitet.

Stellt der Arbeitgeber das Gerät für die dienstliche Nutzung, kann er im Rahmen des Direktionsrechts auch Art und Umfang seiner Nutzung vorschreiben. Anders ist dies bei der dienstlichen Nutzung von privaten Geräten des Arbeitnehmers: Das Privateigentum des Arbeitnehmers unterliegt nicht der Dispositionsbefugnis des Arbeitgebers. Einseitige Vorgaben des Arbeitgebers über die Nutzung solcher Geräte sind unzulässig und damit unwirksam.

2. Arbeitsvertrag

Arbeitgeber und Arbeitnehmer können Umfang und Kontrolle der Nutzung mobiler Geräte in einer Vereinbarung detailliert regeln.

Eine solche Regelung ist allerdings nicht erzwingbar und muss zwischen Arbeitgeber und Arbeitnehmer ausgehandelt werden. Zudem ist die Änderung solcher Vereinbarungen mit einem hohen administrativen Aufwand verbunden, da jede Vereinbarung individuell angepasst werden muss. Wird, wie meist üblich, der Text der Vereinbarung mehrfach, zum Beispiel für mehrere Arbeitnehmer, verwendet, unterliegt er der sogenannten AGB-Kontrolle. Jeder unangemessene Eingriff in Rechtspositionen des Arbeitnehmers ist dann unwirksam, mit der Folge, dass ein regelungsloser Zustand eintritt, den der Arbeitgeber gerade vermeiden sollte.

3. Regelung durch Betriebsvereinbarung

Bei Bestehen eines Betriebsrates ist die Betriebsvereinbarung das Mittel der ersten Wahl zur Regelung der Nutzung mobiler Geräte. Anders als bei einer vertraglichen Regelung haben die Verhandlungspartner hier wesentlich weiteren Gestaltungsspielraum. Zudem wirken Änderungen einer Betriebsvereinbarung automatisch auf alle Arbeitsverhältnisse, was den administrativen Aufwand bei Anpassungen gering hält.

Mitwirkungsrechte des Betriebsrats

Der Arbeitgeber muss den Betriebsrat bei der Einführung der Nutzung mobiler Geräte und bei jeder Änderung in diesem Bereich von Anfang an miteinbeziehen.

1. Mitbestimmung

Moderne Smartphones ermöglichen eine Überwachung des Nutzers. Die Einführung und Anwendung technischer Einrichtungen zur Überwachung von Verhalten und Leistung der Arbeitnehmer ist nach § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz mitbestimmungspflichtig und zwar unabhängig davon, ob eine Überwachung beabsichtigt oder überhaupt gewollt ist. Die bloße technische Möglichkeit der Überwachung reicht aus, um das Mitbestimmungsrecht des Betriebsrates auszulösen.

Da die Nutzung mobiler Geräte auch die Ordnung des Betriebes und das Verhalten der Arbeitnehmer im Betrieb betrifft, ist die Einführung auch nach § 87 Abs. 1 Nr. 1 Betriebsverfassungsgesetz mitbestimmungspflichtig.

Das Mitbestimmungsrecht des Betriebsrates ist zwingend. Der Arbeitgeber kann die beabsichtigte Maßnahme nur einvernehmlich mit dem Betriebsrat regeln. Eine Durchsetzung der Maßnahme gegen den Willen des Betriebsrates ist nicht möglich. Lässt sich eine Einigung nicht herstellen, steht Arbeitgeber und Betriebsrat der Weg zur Einigungsstelle offen, deren Spruch für beide Parteien bindend ist.

Das Mitbestimmungsrecht des Betriebsrates ist weit. Es erfasst Art und Weise sowie den Umfang der beabsichtigten Maßnahme. Damit unterliegen insbesondere die Regelungen über Vollzug und Kontrolle des Datenzugriffs der Mitbestimmung des Betriebsrates. Stellt sich ein eingeführtes Prozedere als untauglich heraus, müssen Änderungen mit dem Betriebsrat abgestimmt werden.



Foto: © Petrovich9/istock.com

2. Arbeitszeitgesetz

Erfahrungsgemäß stehen Betriebsräte Betriebsvereinbarungen über die Nutzung mobiler Geräte im Unternehmen mitunter kritisch gegenüber. Neben den divergierenden Interessen im Hinblick auf die Überwachung des Datenzugriffs bereiten die gesetzlichen Bestimmungen des Arbeitszeitgesetzes Probleme. Beantwortet der Arbeitnehmer beispielsweise abends von zu Hause aus eine dienstliche E-Mail, ist die hierfür aufgewendete Zeit zu vergüten, jedenfalls dann, wenn der Arbeitgeber keine anderweitige Regelung getroffen hat. Außerdem handelt es sich um Arbeitszeit im Sinne des Arbeitszeitgesetzes, die bei der Ermittlung der höchstzulässigen werktäglichen Arbeitszeit zu berücksichtigen ist.

Der Betriebsrat hat nach § 80 Abs. 1 Betriebsverfassungsgesetz die Einhaltung der Arbeitszeitregelungen nach dem Arbeitszeitgesetz, den einschlägigen Tarifverträgen und Betriebsvereinbarungen zu überwachen. Er muss nachvollziehen, ob die regelmäßige werktägliche Arbeitszeit und die wöchentliche Höchstarbeitszeit eingehalten werden. Der Einsatz von mobilen Geräten eröffnet den Mitarbeitern die Möglichkeit, dienstliche Aufgaben auch außerhalb ihrer regelmäßigen Arbeitszeit im Betrieb zu erledigen. Dadurch verschwimmen die Grenzen zwischen privater Freizeit und dienstlicher Arbeitszeit, eine Kontrolle der höchstzulässigen werktäglichen Arbeitszeit wird erschwert. Hier können Pragmatismus und wechselseitiges Vertrauen helfen, damit starre gesetzliche Regelungen einen sinnvollen und von den Arbeitnehmern erwünschten Einsatz moderner Technologien nicht verhindern.

Kontrollrechte und Schutz der Privatsphäre

Ein Arbeitgeber hat ein legitimes Interesse daran, in bestimmten Fällen auf dienstlich genutzte Geräte zuzugreifen. Der Arbeitgeber muss die Möglichkeit haben, Daten von einem Gerät zu löschen, wenn dieses verloren geht oder gestohlen wird. Ein Arbeitgeber wird in bestimmten Fällen den Inhalt eines Gerätes kontrollieren wollen, etwa um sicherzustellen, dass Sicherheitsrichtlinien zur Vermeidung von Malware eingehalten werden.

Gesetz und Rechtsprechung setzen den Zugriffsmöglichkeiten Grenzen. § 202a Strafgesetzbuch verbietet es, auf fremde Daten zuzugreifen, wenn dabei Sicherheitsmechanismen, zum Beispiel ein Passwort, überwunden werden. Ein Systemadministrator darf also nicht ein vom Arbeitnehmer eingerichtetes Passwort umgehen, um den Inhalt eines Geräts zu überprüfen.

Die (noch) geltende Regelung zum Arbeitnehmerdatenschutz in § 32 Bundesdatenschutzgesetz setzt der Nutzung von Daten eines Arbeitnehmers enge Grenzen, wenn diese Nutzung nicht unmittelbar für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist.

Das auf eine Entscheidung des Bundesverfassungsgerichts aus dem Jahr 2008 zurückgehende Computergrundrecht gewährleistet eine grundsätzliche Vertraulichkeit von IT-Systemen. Hierzu zählen auch mobile Geräte.

Ergänzt werden diese Regelungen durch das allgemeine Persönlichkeitsrecht des Arbeitnehmers, das es dem Arbeitgeber verbietet, Arbeitnehmer über Gebühr zu überwachen.

Dieses Mosaik aus Regelungen schafft für Arbeitgeber ein hohes Maß an Rechtsunsicherheit, welche dadurch verstärkt wird, dass insbesondere Eingriffe in das Persönlichkeitsrecht des Arbeitnehmers unter dem Vorbehalt einer Interessenabwägung stehen, deren Ergebnis auch vom subjektiven Empfinden des Gerichts abhängen kann.

Ein rechtswidriger Zugriff des Arbeitgebers auf Geräte des Arbeitnehmers löst Unterlassungs- und Schadenersatzansprüche des Arbeitnehmers aus. Die rechtswidrig gewonnen Erkenntnisse dürfen vor Gericht nicht verwertet werden.

Sichere Zugriffs- und Kontrollmöglichkeiten setzen eine sorgfältige technische und juristische Gestaltung voraus:

Technisch wird ein Zugriff umso leichter, je sauberer die Trennung zwischen beruflicher und privater Sphäre auf dem Gerät vollzogen wird. Wenn etwa technisch vermieden werden kann, dass Unternehmensdaten lokal auf einem mobilen Gerät gespeichert werden, ist ein physischer Zugriff des Arbeitgebers auf das



Gerät unter Umständen entbehrlich. Bei einem Verlust genügt es, den Zugang des Geräts zum Server des Arbeitgebers zu sperren.

Rechtlich sollten die Zugriffs- und Kontrollrechte in einer Betriebsvereinbarung oder einer Ergänzung zum Arbeitsvertrag möglichst exakt geregelt werden. Auch hier gelten natürlich die bereits dargestellten AGB-rechtlichen Grenzen.

Je genauer die Voraussetzungen und die Grenzen von Eingriffen (z. B. dem Recht des Arbeitgebers, bei Gefahr im Verzug ein Gerät zurückzusetzen – Remote Wipe) geregelt sind, desto eher hält die Regelung einer gerichtlichen Überprüfung stand. Solange es keine Präzedenzentscheidungen der Arbeitsgerichte in diesem Bereich gibt, verbleibt freilich ein gewisses Maß an Rechtsunsicherheit.

Risikoverteilung im Schadensfall

Bei einer dienstlichen Nutzung privater Geräte ist es für Arbeitgeber und Arbeitnehmer eine ganz wesentliche Frage, ob und in welchem Umfang der Arbeitgeber bei Verlust oder Beschädigung des Geräts Ersatz zu leisten hat.

Anders als die Schutzpflichten des Arbeitgebers für Leben und Gesundheit des Arbeitnehmers sind Schutzpflichten des Arbeitgebers für Vermögensgegenstände des Arbeitnehmers nicht gesetzlich geregelt. Eine Schutzpflicht für berechtigterweise in den Betrieb eingebrachte Sachen des Arbeitnehmers wird aus der allgemeinen Fürsorgepflicht des Arbeitgebers gegenüber dem Arbeitnehmer hergeleitet. Für das Bestehen arbeitgeberseitiger Schutzpflichten kommt es maßgeblich darauf an, ob der vom Arbeitnehmer eingebrachte Privatgegenstand in einem inneren Zusammenhang zu der von ihm geschuldeten Arbeitsleistung steht oder nicht. Hierzu hat sich eine kaum mehr zu überblickende Kasuistik in der Rechtsprechung herausgebildet.

Keine Schutzpflichten bestehen für Vermögensgegenstände des Arbeitnehmers, die mit der Arbeitsleistung in keinem Zusammenhang stehen, etwa einem zu Privatzwecken auf einer Dienstreise mitgeführten Fotoapparat oder iPod. Etwas anderes kann

ausnahmsweise dann gelten, wenn das Mitführen solcher Gegenstände, betriebsüblich, gestattet oder dienstlich erwünscht ist.

Für Gegenstände, die zur Durchführung der Arbeitsleistung, aber auch zum Erreichen der Arbeitsstätte erforderlich sind, hat der Arbeitgeber für alle betriebsüblichen Gefahren Vorkehrungen und Sicherungsmaßnahmen zu treffen, beispielsweise den Abschluss entsprechender Versicherungen oder die Bereitstellung von Verwahrungsmöglichkeiten. Welche Vorkehrungen der Arbeitgeber im Einzelnen zu treffen hat, hängt von den Umständen des Einzelfalles ab.

Schwieriger ist die Frage zu beantworten, wenn die vom Arbeitnehmer eingebrachten Privatgegenstände für die Erbringung der Arbeitsleistung nicht notwendig, ihr aber dienlich sind. Dies dürfte in der Praxis wohl der Regelfall sein. Obwohl das Arbeiten ohne iPad und Co. für viele kaum noch vorstellbar ist, sind diese Geräte der Erbringung der Arbeitsleistung zwar dienlich, für sie aber nicht notwendig.

Bei Vermögensgegenständen des Arbeitnehmers, die der Arbeitsleistung des Arbeitnehmers „nur“ dienlich sind, entstehen Schutzpflichten des Arbeitgebers regelmäßig dann, wenn der Arbeitgeber den Einsatz dieser Vermögensgegenstände anordnet oder zumindest duldet.

Das während einer Dienstreise gestohlene private Notebook des Arbeitnehmers muss der Arbeitgeber jedenfalls dann ersetzen, wenn er dem Arbeitnehmer überhaupt kein mobiles Endgerät zur Verfügung stellt und der Arbeitnehmer sein privates Notebook nur mitgeführt hat, weil ihm das Arbeiten während der Dienstreise unmöglich wäre. In diesem Falle war das private Notebook für die Erbringung der Arbeitsleistung notwendig.

Gleiches gilt, wenn der Arbeitgeber die Nutzung des privaten Notebooks zu dienstlichen Zwecken duldet. Hier erfolgte die Nutzung im unterstellten Einverständnis des Arbeitgebers.

Zieht man die Rechtsprechung der Arbeitsgerichte zur dienstlichen Nutzung privater Pkws heran, gilt etwas anderes dann, wenn der Arbeitgeber dem Arbeitnehmer für die Nutzung des

privaten Geräts einen angemessenen finanziellen Ausgleich bezahlt.

Eine andere Frage ist, wie sich ein Mitverschulden des Arbeitnehmers bei Beschädigung oder Verlust des Geräts auswirkt. Hat der Arbeitgeber auch dann Ersatz zu leisten, wenn der Arbeitnehmer sich beim Umgang mit seinem Gerät fahrlässig verhalten hat, dieses etwa aus Nachlässigkeit im Zug hat liegen lassen?

Es spricht vieles dafür, hier die Grundsätze des Arbeitnehmerhaftungsprivilegs analog heranzuziehen. Hiernach haftet ein Arbeitnehmer nicht, wenn er sich bei Verrichtung einer dienstlichen Tätigkeit leicht oder einfach fahrlässig verhält. Nur bei Vorsatz und grober Fahrlässigkeit trifft den Arbeitnehmer eine eigene persönliche Haftung. Nichts anderes kann für das Mitverschulden des Arbeitnehmers an einem Schaden gelten, für den der Arbeitgeber aufgrund seiner Fürsorgepflicht einzustehen hat.

Schutz von Rechten Dritter

Vorsicht ist auch geboten, wenn Daten auf ein mobiles Gerät kopiert werden, an dem Dritte eigene Rechte haben. Dies können urheberrechtlich geschützte Informationen (z. B. Software) sein, personenbezogene Daten oder Daten, die ein Betriebs- oder Geschäftsgeheimnis enthalten oder von einer Geheimhaltungsvereinbarung erfasst sind.

Bei Software stellt sich insbesondere die Frage, ob eine Unternehmenslizenz es gestattet, die Software auch auf einem privaten Gerät des Arbeitnehmers zu installieren, wenn dieser das private Gerät beruflich nutzen möchte. Mitunter regeln Lizenzbestimmungen, dass eine Installation der Software nur auf Computern erfolgen darf, die im Eigentum und Besitz des Lizenznehmers (also des Arbeitgebers) stehen. Dies schließt eine Installation auf privaten Geräten aus. Häufig lohnt sich hier aber eine juristische Überprüfung der Lizenzbedingungen. Viele bei US-Software-Herstellern üblichen Lizenzbeschränkungen sind nach deutschem AGB-Recht unwirksam.

Eine andere Frage ist, ob ein Arbeitnehmer personenbezogene Daten (z. B. Kunden oder Lieferantendaten) auf ein privates Device kopieren darf. Ein Arbeitnehmer ist datenschutzrechtlich im Rahmen seiner dienstlichen Tätigkeit Teil der „verantwortlichen Stelle“, verarbeitet diese Daten also auf Grundlage der für sein Unternehmen geltenden datenschutzrechtlichen Ermächtigung. Diese Ermächtigung gilt nicht für den Arbeitnehmer als Privatperson. Eine Datenübermittlung an Privatpersonen bedürfte einer eigenen datenschutzrechtlichen Rechtfertigung, die in der Regel nicht vorliegt.

Teilweise wird hier vorgeschlagen, zwischen dem Arbeitnehmer und dem Unternehmen eine Auftragsdatenverarbeitung nach § 11 Bundesdatenschutzgesetz zu vereinbaren. Wir halten diese Lösung nicht für sinnvoll, da eine Privatperson nicht verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes sein kann. Die Regelungen zur Auftragsdatenverarbeitung sind nicht für die Datenverarbeitung durch Privatpersonen gemacht.

Die Lösung liegt auch hier in einer konsequenten Trennung der privaten und beruflichen Sphäre. Wenn ein Arbeitnehmer das Gerät privat nutzt, sollte ein Zugriff auf personenbezogene Unternehmensdaten ausgeschlossen sein.

Fazit

Die mit der dienstlichen Nutzung privater Geräte des Arbeitnehmers verbundenen rechtlichen Unsicherheiten haben das Potenzial, das Arbeitsverhältnis im Streitfalle nachhaltig zu belasten. Arbeitgeber und Arbeitnehmer sind daher gut beraten, die dienstliche Nutzung von Privatgegenständen des Arbeitnehmers, deren Umfang und die hieraus resultierenden Pflichten vertraglich zu regeln. Dies betrifft nicht nur die Bereitstellungs- und Ersatzpflichten der Parteien sondern auch die jeweiligen Nebenpflichten im Umgang mit diesen Gegenständen.

Wichtiger noch als die rechtliche ist die sorgfältige technische Umsetzung. Die wesentlichen rechtlichen Risiken resultieren aus der Vermischung von privater und beruflicher Sphäre auf einem Gerät. Technische Lösungen, die es erlauben, diese Sphären zu trennen (z. B. eine Virtualisierung, Terminallösungen, zentrale Datenhaltung etc.) verkleinern die rechtlichen Probleme erheblich. Im einen oder anderen Fall wird dies freilich mit einem Verlust von Bedienkomfort einhergehen. Es ist bereits zu beobachten, dass die Anbieter technischer Mobile-Device-Management-Lösungen die rechtlichen Fallstricke erkannt haben und mehr und mehr Lösungen entwickeln, die Bedienkomfort und Rechtssicherheit vereinen.

Literatur

- Söbbing, T.; Müller, N. R.: Bring your own Device: Haftung des Unternehmens für urheberrechtsverletzenden Inhalt. ITRB 2012, 15–17.
- Koch, F.: Arbeitsrechtliche Auswirkungen von „Bring your own Device“. ITRB 2012, 35–39.
- Söbbing, T.; Müller, N. R.: Bring your own Device. Strafrechtliche Rahmenbedingungen. ITRB 2011, 263–266.
- Bissels, A.; Domke, C.; Wisskrichen, G.: BlackBerry & Co.: Was ist heute Arbeitszeit?. DB 2010, 2052–2055.
- Conrad, I.; Schneider, J.: Einsatz von „privater IT“ im Unternehmen – kein privater USB-Stick, aber „Bring your own Device“ (BYOD)?. ZD 2011, 160–166.

Autoren

Thorsten Walter

berät Unternehmen und Führungskräfte in allen Bereichen des individuellen und kollektiven Arbeitsrechts und der betrieblichen Altersversorgung. Er ist Fachanwalt für Arbeitsrecht und Partner der Kanzlei Bartsch Rechtsanwälte.

Joachim Dorschel

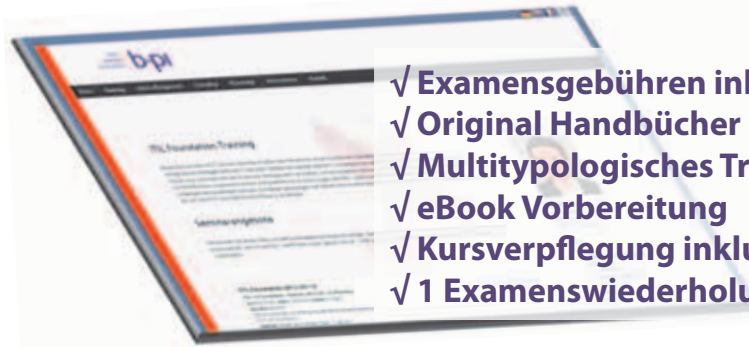
berät mittelständische und größere Unternehmen im In- und Ausland in allen Fragen des IT-Rechts. Zu den Schwerpunkten gehören IT-Compliance, Datenschutz und Vertragsgestaltung. Herr Dorschel ist Rechtsanwalt und Partner der Kanzlei Bartsch Rechtsanwälte.

There's a way to do it better*

Service Management nach ITIL®

Projektmanagement nach PRINCE2®

Erwerben Sie Expertenkenntnisse in den 2 wichtigsten Disziplinen für die Bereitstellung und das Management von IT Services!



- ✓ Examensgebühren inklusive
- ✓ Original Handbücher inklusive
- ✓ Multitypologisches Training
- ✓ eBook Vorbereitung
- ✓ Kursverpflegung inklusive
- ✓ 1 Examenswiederholung inklusive

Behalten Sie den Überblick.

Gewinnen Sie einen Rundflug

für Sie und eine Begleitperson Ihrer Wahl im Rhein-Main oder Rhein-Ruhr Gebiet

Sichern Sie sich Ihre Chance.

Besuchen Sie unsere Gewinnspiel-Seite <http://win.b-pi.com/de>



Unter allen Teilnehmern mit der richtigen Antwort verlosen wir einen einstündigen Rundflug mit dem Flugzeug. Der Gewinner wird am 30. Juni 2012 gezogen. Die Terminvereinbarung für den Rundflug erfolgt individuell nach Absprache.

Die Teilnahmebedingungen können auf unserer Gewinnspiel-Seite eingesehen werden.



ITIL® Expert Intensiv

ITIL® Foundation	895,- €*
Service Strategy	1.195,- €*
Service Design	1.195,- €*
Service Transition	1.195,- €*
Service Operation	1.195,- €*
Cont. Service Improvement	1.195,- €*
Managing across the Lifecycle	1.495,- €*

18.06 - 19.09.12 in **Köln**
20.08 - 31.10.12 in **Frankfurt a.M.**
08.10 - 19.12.12 in **Berlin**

7.595,-€* Paketpreis

b-pi ist durch die weltweit verantwortliche APM Group aus Großbritannien als Trainingsorganisation für ITIL® Kurse akkreditiert (ATO).
 Alle Seminare werden von in ITIL® akkreditierten Trainern unter Einbeziehung ihrer langjährigen Erfahrung im Service Management vermittelt.



PRINCE2® Practitioner

PRINCE2® Foundation	1.195,- €*
PRINCE2® Practitioner	1.495,- €*

09.07 - 13.07.12 in **Frankfurt a.M.**
06.08 - 10.08.12 in **Berlin**
27.08 - 31.08.12 in **Köln**
17.09 - 21.09.12 in **Frankfurt a.M.**
22.10 - 26.10.12 in **Berlin**
05.11 - 09.11.12 in **Köln**
10.12 - 14.12.12 in **Frankfurt a.M.**

2.445,-€* Paketpreis

Das akkreditierte PRINCE2® Training wird veranstaltet von unserem Partner Bizness Académie SAS, akkreditierte Trainings-Organisation (ATO) unter Lizenz der APMG-International und daher autorisiert, PRINCE2 Trainings durchzuführen, die zum offiziellen Examen führen.



* Alle Preise sind Nettopreise und verstehen sich zzgl. gesetzlicher Mehrwertsteuer.



best-practice innovations GmbH
 Berrenrath Str. 188c, D-50937 Köln
 Tel.: +49 221 9643463-0
 e-mail: info@b-pi.com
 Website: www.b-pi.com/de

Wir sind ein mittelständisches Trainings- und Beratungsunternehmen in den Bereichen IT-Service-Management, Projekt-Management, IT-Governance. Auf unsere Kompetenzen vertrauen mittelständische und große Unternehmen genauso wie öffentliche Organisationen und Hochschulen – national wie international.