1/2014

CHECKLISTE
Bring Your Own Device
Hans-Jürgen Pollirer

DATENSCHUTZ KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Der betriebliche Datenschutzbeauftragte

Hans-Jürgen Pollirer

Interview mit Andrea Jelinek

Rainer Knyrim, Katharina Schmidt

Praxisprojekt: Datenschutzschulung durch eLearning

Markus Oman, Siegfried Gruber

Was sind personenbezogene Daten?

Viktoria Haidinger

Datenschutz vor Gericht

Ernst M. Weiss

ISSN 2313-5409

dako.manz.at

MANZ

P.b.b. Verlag Manz 1230 Wien, Gutheil Schoder Gasse 17

Hans-Jürgen Pollirer
Geschäftsführer der Secur-Data Betriebsberatungs-GmbH

Checkliste – Bring Your Own Device (BYOD)

Das private Smartphone, Tablet und Internetdienste beruflich nutzen. Mitarbeiter wollen ihre privaten Geräte und Software auch im Beruf einsetzen. Der Trend ist geprägt von einer Vielfalt an verschiedenen Geräten mit unterschiedlichen Betriebssystemen. Der Beitrag zeigt die Vor- und Nachteile auf, die sich für Mitarbeiter und Unternehmen ergeben. Prüffragen in Form einer Checkliste unterstützen bei der Einführung einer BYOD-Richtlinie.

Alltag in der Mobility-Landschaft

Mit der sog „Consumerisation der IT" löst sich die Grenze zwischen beruflicher und privater IT-Nutzung auf, dh, Systeme, Programme und Dienste werden sowohl im beruflichen als auch im privaten Bereich verwendet. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) führt in seinem „Überblickspapier Consumerisation und BYOD" folgende **Einsatzbeispiele** an:

- Mitarbeiter wollen ihre privaten Smartphones und Tablets für dienstliche

E-Mails, Termine und sonstige dienstliche Tätigkeiten nutzen.
- Mitarbeiter sind privat an bestimmte Programme, wie zB das Grafikbearbeitungsprogramm GIMP, gewöhnt und möchten diese auch in ihrem Beruf einsetzen.
- Mitarbeiter benutzen privat Internetdienste, wie zB Dropbox zur Speicherung von Daten in der Cloud oder Werkzeuge wie Doodle, um Termine abzustimmen, und möchten diese Dienste auch beruflich nutzen.

Geprägt war die Mobility-Landschaft lange Zeit durch BlackBerry-Geräte, die höchste Sicherheit und Stabilität garantierten. In der Zwischenzeit haben BlackBerry-Geräte an Attraktivität stark verloren und iPhones und iPads mit dem Betriebssystem iOS haben ihren Einzug in die Unternehmen gefunden. Die gleiche Feststellung trifft auch auf Android-Geräte zu, allerdings verbunden mit dem Problem, dass die verschiedenen Hersteller dieses Betriebssystem um eigene Komponenten ergänzen, sodass von einer einheitlichen Betriebssystemumgebung keine Rede sein kann. Die **Vielfalt** an verschiedenen **Geräten** mit unterschiedlichen **Betriebssystemen** erhöht den Verwaltungsaufwand in der IT-Abteilung wesentlich.

Mit dem Begriff „**Consumerisation**“ verwandt ist der mit der Abkürzung **BYOD** verbundene Trend. Hier nutzen die Mitarbeiter ihre privaten Geräte (Notebooks, Tablets und Smartphones) nicht nur für private, sondern auch für berufliche Zwecke. Sie greifen damit auf die Server des Unternehmens zu und speichern bzw verarbeiten firmeneigene Daten auf ihren persönlichen Geräten. Die Besonderheit von BYOD liegt in der Tatsache begründet, dass sich die Geräte im Eigentum der Mitarbeiter befinden, auch wenn sich Unternehmen manchmal an den Kosten für die Anschaffung und den Betrieb beteiligen.

Folgt man den Ergebnissen verschiedener Umfragen, so haben den Trend zu BYOD eindeutig die Anwender ausgelöst, weil sie gerne die Letztversionen ihrer Smartphones, Tablets und Notebooks verwenden und es wesentlich bequemer ist, nur ein Gerät anstatt zwei Geräte mitzuführen. Darüber hinaus sind die privaten Geräte in der Regel oft moderner ausgestattet und leistungsfähiger als diejenigen, die vom Unternehmen zur Verfügung gestellt werden.

BYOD ist bequem für den Anwender, für das Unternehmen stellen sich jedoch eine Reihe von arbeits-, datenschutz- und urheberrechtlichen Fragen.

Vor- und Nachteile von BYOD

Der Einsatz von BYOD kann aus der Sicht des Unternehmens Vorteile mit sich bringen. Allerdings gibt es auch eine Reihe von Nachteilen, die bei der Entscheidung, ob BYOD eingesetzt werden soll oder nicht – sofern diese Entscheidung nicht schon längst durch einen schleichenden und nicht strategisch bestimmten Einsatz von BYOD obsolet geworden ist –, zu berücksichtigen sind.

Zu den **Vorteilen** aus Sicht des Unternehmens zählen:
- Kosten für neue Hardware können eingespart werden.
- Mitarbeiterinnen und Mitarbeiter sind besser motiviert, wenn sie aktuelle Geräte für ihre Arbeit einsetzen können.
- Mitarbeiterinnen und Mitarbeiter können ihre Geräte selbst aussuchen, ohne auf bestehende Hard- und Softwareangebote des Arbeitgebers angewiesen zu sein.
- Die Notwendigkeit, mehrere mobile Geräte mitzuführen, entfällt.
- Stärkere Bindung der Mitarbeiter an das Unternehmen.
- Entlastung der IT-Abteilung durch Wegfall des Supports für die mobilen Geräte.

Diesen Vorteilen stehen folgende **Nachteile** entgegen:
- BYOD ist nicht für alle Arbeitsplätze anwendbar.
- Kompatibilitätsprobleme können auftreten.
- Aufwendige Zugriffskontrollmechanismen werden notwendig.
- Bedingt durch technische Diskussionen unter den Mitarbeitern kann es zu Arbeitszeitverlust kommen.
- Wichtige Sicherheitsvorgaben, insb die strikte Trennung zwischen privaten und beruflichen Daten, sind ohne zusätzliche kostenpflichtige Software (Mobile Device-Management-Programme) nicht umsetzbar.
- Eventuell müssen aus Sicherheitsgründen Umbauten der IT-Infrastruktur (zusätzliche Server für den Remote-Zugang, Trennung von Netzwerkbereichen) erfolgen.
- Bei Beschädigung oder Verlust des privaten mobilen Geräts haftet grundsätzlich der Arbeitgeber, sofern der Schaden aufgrund der dienstlichen Tätigkeit entstanden ist. Dadurch können hohe Aufwände für die Reparatur oder Wiederbeschaffung entstehen.
- Weitere Kosten können für zusätzliche Softwarelizenzen anfallen, da viele Apps nur dann kostenlos verwendet werden dürfen, wenn sie ausschließlich für private Zwecke genutzt werden.
- Es besteht ein hohes Datensicherheitsrisiko.

Prüffragen

Damit die Einführung von „Bring Your Own Device“ nicht zu „Bring Your Own Dilemma“ oder sogar „Bring Your Own Disaster“ wird, bedarf es einer unternehmensweiten **BYOD-Strategie** mit einer klaren **BYOD-Richtlinie** sowie einer Auseinandersetzung mit diversen rechtlichen Fragen, vor allem aus den Bereichen Arbeitsrecht, Datenschutzrecht und Urheberrecht. Die nachfolgende Checkliste soll den für die Einführung von BYOD zuständigen Personenkreis bei der Überprüfung der notwendigen Maßnahmen unterstützen:

Prüffrage	nicht anwendbar	erfüllt	nicht erfüllt
Prüfpunkt 1 – BYOD-Richtlinie			
Frage 1: Ist eine unternehmensweite BYOD-Richtline vorhanden? ***Anmerkung:** Das größte Problem beim Einsatz von BYOD liegt im Sicherheitsbereich, da die Kontrolle des Unternehmens über die eingesetzte Hardware und Software durchbrochen wird. Es ist daher unbedingt erforderlich, ein Regelwerk zu entwickeln, um dieses hohe Sicherheitsrisiko zu minimieren. Der Inhalt dieser BYOD-Richtlinie ergibt sich aus den folgenden Fragen.*			
Frage 2: Ist eindeutig geregelt, welche Mitarbeiter an BYOD teilnehmen dürfen?			

Prüffrage	nicht anwendbar	erfüllt	nicht erfüllt
Frage 3: Ist eindeutig geregelt, welche mobilen Geräte eingesetzt werden dürfen bzw welche vom Einsatz ausgeschlossen sind?			
Frage 4: Ist eindeutig geregelt, welche Software eingesetzt werden darf bzw welche Software vom Einsatz ausgeschlossen ist? ***Anmerkung:** Damit soll zB die Nutzung von nichtvertrauenswürdigen Cloud-Diensten ausgeschlossen werden.*			
Frage 5: Ist eindeutig geregelt, welche Apps installiert werden dürfen und welche nicht?			
Frage 6: Ist eindeutig geregelt, welche Betriebssysteme zugelassen sind bzw welche nicht zum Einsatz kommen dürfen?			
Frage 7: Ist eindeutig geregelt, welche Informationen mit welchem Schutzbedarf mit den mobilen Geräten verarbeitet werden dürfen? ***Anmerkung:** Denkbar wäre eine Datenklassifikation in 4 Sicherheitsklassen, wie zB Klasse 0 = öffentlich, 1 = geschützt, 2 = geheim und 3 = vertraulich. Anhand dieser Datenklassifikation wäre dann zu definieren, bis zu welcher Klasse mobile Geräte zum Einsatz kommen dürfen.*			
Frage 8: Enthält die BYOD-Richtlinie auch nichttechnische Vorsichtsmaßnahmen, wie zB, ob die mobilen Geräte an Dritte verliehen oder in öffentlichen Bereichen benützt werden dürfen?			
Frage 9: Werden private und betriebliche Daten und Anwendungen getrennt? ***Anmerkung:** Es ist auch darauf zu achten, dass durch Synchronisation/Backup insb von Smartphones oder Tablets mit/auf privaten Computern keine beruflichen Daten auf privaten Geräten gespeichert werden!*			
Frage 10: Ist der Einsatz von Zertifikaten (zB SCEP, Token) auf den Mobilgeräten vorgesehen? ***Anmerkung:** Benutzername und Kennwort sind bei BYOD aufgrund der ungesicherten Umgebung für die Zugangskontrolle kaum ausreichend.*			
Frage 11: Werden verschlüsselte Datencontainer oder ein Information Rights Management (IRM) zum Schutz der betrieblichen Daten eingesetzt?			
Frage 12: Sind die Zugriffsrechte der IT-Abteilung auf die mobilen Geräte eindeutig geregelt?			
Frage 13: Ist der Einsatz einer automatischen Löschfunktion (Wipe) vorgesehen, wenn das Mobilgerät über einen bestimmten Zeitraum nicht am Firmennetzwerk angemeldet war?			
Frage 14: Ist das Vorgehen bei Security Updates geregelt?			
Frage 15: Ist das Vorgehen beim Einspielen von Patches geregelt?			
Frage 16: Ist ein Prozess eingerichtet, der das Vorgehen bei einem Verlust oder Diebstahl eines mobilen Geräts regelt? ***Anmerkung:** Bei Verlust oder Diebstahl eines mobilen Geräts ist eine sofortige Benachrichtigung der IT-Abteilung durch den betroffenen Mitarbeiter unbedingt erforderlich, um den Zugriff auf das mobile Gerät zu sperren und die Daten zu löschen.*			
Frage 17: Ist genau geregelt, wie bei einer Reparatur bzw nach einem Absturz des mobilen Geräts vorzugehen ist?			
Frage 18: Gibt es ein Datensicherheitskonzept für die mobilen Endgeräte? ***Anmerkung:** Das Datensicherheitskonzept sollte genau regeln, wie bei Datenlöschungen (komplette oder partielle Löschung) bzw bei Sperrungen vorzugehen ist.*			
Frage 19: Sind alle mobilen Geräte mit Spam-, Malware und Virenschutz ausgestattet?			
Frage 20: Werden die Mitarbeiter in den Sicherheitsthemen entsprechend geschult?			
Frage 21: Werden alle Daten auf den mobilen Geräten verschlüsselt und entspricht das eingesetzte Verschlüsselungsverfahren dem Stand der Technik?			
Frage 22: Wurde ein Prozess eingerichtet, wie beim Ausscheiden eines Mitarbeiters mit Daten auf seinen mobilen Geräten zu verfahren ist?			
Frage 23: Wird ein Mobile Device-Management-System (MDM) eingesetzt? ***Anmerkung:** Die nachfolgenden Fragen von 24 bis 43 beziehen sich auf die Sicherheitsmerkmale des MDM, die bei der Auswahl eines solchen Systems zu beachten sind.*			
Frage 24: Weist das MDM Mandantenfähigkeit auf?			
Frage 25: Werden die unterschiedlichsten mobilen Geräte unterstützt?			
Frage 26: Ist eine Übertragung bestehender Unternehmensrichtlinien auf die mobilen Geräte möglich?			
Frage 27: Erfolgt eine Inventarisierung der Mobilfunkumgebung (mit automatischer Geräteerkennung)?			
Frage 28: Erfolgt eine Überwachung der Mobilfunkkosten, insb von Roamingkosten?			
Frage 29: Ist eine plattformübergreifende Migration der Daten zu den mobilen Geräten möglich (zB Übernahme Adressbuch, Anwendungen, Einstellungen)?			
Frage 30: Erfolgt eine fortlaufende Sicherung der Daten auf den mobilen Endgeräten?			
Frage 31: Ist der Einsatz von Anti-Malware vorgesehen?			
Frage 32: Gibt es eine Jailbreak- und Rootingerkennung für alle bekannten Exploits?			
Frage 33: Verfügt das MDM über einen Spamfilter?			
Frage 34: Erfolgt eine Verschlüsselung der mobilen Geräte und eventueller Speicherkarten?			
Frage 35: Enthält das MDM eine White-List und Black-List für mobile Applikationen?			
Frage 36: Wird die Installation von Zertifikaten auf beliebig vielen Devices unterstützt?			
Frage 37: Ist eine Verwaltung der Sicherheitsrichtlinien enthalten?			
Frage 38: Erfolgt eine Verwaltung der Applikationen?			

Prüffrage	nicht anwendbar	erfüllt	nicht erfüllt
Frage 39: Enthält das MDM eine Echtzeitremoteunterstützung oder Helpdesklösung?			
Frage 40: Enthält das MDM eine Konfigurationsverwaltung?			
Frage 41: Verfügt das MDM über eine Sperr- und Löschmöglichkeit für mobile Endgeräte, Funktionen und Speichermedien?			
Frage 42: Ist eine Lokalisierung von verloren gegangenen mobilen Geräten per GPS möglich?			
Frage 43: Verfügt das MDM über Remote Wipe?			
Prüfpunkt 2 – Arbeitsrecht			
Frage 44: Wurde vor Einführung von BYOD eine Betriebsvereinbarung (BV) abgeschlossen oder bei nicht eingerichtetem Betriebsrat die Zustimmung jedes einzelnen Mitarbeiters nach § 10 AVRAG eingeholt? ***Anmerkung:** Grundsätzlich eignet sich BYOD aufgrund der Verknüpfung des privaten mobilen Geräts mit dem IT-System des Arbeitgebers zur Überwachung und Kontrolle des Mitarbeiters. Für die Einführung von Systemen, die objektiv geeignet sind, das Verhalten oder die Leistung des Mitarbeiters zu kontrollieren, ist nach den Bestimmungen des § 96 Abs 1 Z 3 ArbVG der Abschluss einer Betriebsvereinbarung unumgänglich.*			
Frage 45: Regelt die BV die Kostenfrage in Bezug auf Beschaffung und Betriebskosten der mobilen Geräte? Gibt es eine Regelung zur Zulässigkeit oder Verbot von Roaming und Tragung von Roamingkosten in der BV? Wurde die Kostenregelung steuerlich geprüft?			
Frage 46: Ist in der BV eine Bestimmung enthalten, die das Risiko der Überschreitung der zulässigen Arbeitszeit oder ausufernder Überstunden unterbindet? ***Anmerkung:** Da der Mitarbeiter sein privates Mobilgerät in der Regel außerhalb seiner Arbeitszeit kaum ausschalten wird, so wie er es mit einem dienstlichen Gerät tun würde, kann es schon beim Lesen einer betrieblich verursachten E-Mail zu einer Verletzung des Arbeitszeitgesetzes (AZG) bzw Arbeitsruhegesetzes (ARG) kommen. Weiters ist zu beachten, dass das mobile Arbeiten Überstundenforderungen nach sich ziehen kann (selbst bei All-in-Arbeitsverträgen darf der Mitarbeiter durch das mobile Arbeiten nicht schlechtergestellt werden, als wenn er keine Überstundenpauschale hätte).*			
Frage 47: Enthält die BYOD-Richtlinie die detaillierte Vorgehensweise bei Verlust des mobilen Geräts?			
Frage 48: Ist in der BV klargestellt, wer bei Verlust des mobilen Endgeräts für die Ersatzbeschaffung, die damit verbundenen Kosten verantwortlich ist bzw für etwaige Schäden haftet?			
Frage 49: Ist die Zugriffsberechtigung der IT-Abteilung auf die in den mobilen Geräten gespeicherten Daten – gegebenenfalls auch einschließlich der persönlichen Daten des Mitarbeiters – sowie Anwendungen in der BV geregelt?			
Frage 50: Enthält die BYOD-Richtlinie entsprechende Regelungen, die den Mitarbeiter verpflichtet, entsprechende Schutzmaßnahmen gegen Viren und sonstige Schadsoftware zu ergreifen?			
Frage 51: Ist in der BYOD-Richtlinie geregelt, wie der unbefugte Zugriff auf das mobile Gerät verhindert werden kann?			
Frage 52: Enthält die BYOD-Richtlinie eine Bestimmung, dass der Mitarbeiter nur jene Hardware und Software einsetzen darf, die vom Unternehmen zugelassen ist?			
Frage 53: Wird in der BV auch auf mögliche Sanktionen bei Verstoß gegen die BYOD-Richtlinie hingewiesen?			
Frage 54: Enthält die BYOD-Richtlinie auch Regelungen in Bezug auf die zu treffenden Maßnahmen bei Beendigung des Arbeitsverhältnisses?			
Prüfpunkt 3 – Urheberrecht			
Frage 55: Wurden sämtliche Unternehmenslizenzen darauf überprüft, ob von ihnen auch die Nutzung auf den mobilen Geräten der Mitarbeiter abgedeckt wird? ***Anmerkung:** Da die meisten Software-Anbieter für die gewerbliche und die private Nutzung von Software unterschiedliche Lizenzbedingungen vorsehen, ist diese Frage dringend zu klären, damit für das Unternehmen keine Haftungsrisken entstehen.*			
Frage 56: Wurden die Mitarbeiter in der BYOD-Richtlinie darauf hingewiesen, dass ihre private Software grundsätzlich nicht zu Betriebszwecken verwendet werden soll? ***Anmerkung:** Diese Frage betrifft vor allem Apps, deren kostenlose Nutzung in der Regel nur für den privaten Einsatz vorgesehen ist.*			
Frage 57: Wurden die Mitarbeiter darauf hingewiesen, dass sie keinesfalls „Raubkopien" zu betrieblichen Zwecken verwenden dürfen?			
Prüfpunkt 4 – Datenschutz			
Frage 58: Sind private und betriebliche Daten strikt getrennt? ***Anmerkung:** Diese und alle weiteren Prüffragen beziehen sich auf die datenschutzrechtlichen Anforderungen des § 14 DSG 2000. Demnach ist der Unternehmer (= Auftraggeber iSd DSG 2000) als Herr der Daten verpflichtet, angemessene Datensicherheitsmaßnahmen zu treffen, um sicherzustellen, dass Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind.* *Der Vollständigkeit halber sei darauf hingewiesen, dass der Auftraggeber noch eine Vielzahl weiterer datenschutzrechtlicher Anforderungen erfüllen muss, von der Einhaltung der Qualitätsgrundsätze des § 6 DSG 2000 bis zur Wahrung der Rechte des Betroffenen in Bezug auf Auskunft, Richtigstellung oder Löschung und Widerspruch (§§ 26–28 DSG 2000), deren Behandlung den Rahmen dieser Checkliste sprengen würde.*			
Frage 59: Sind die Mitarbeiter angewiesen, ihre mobilen Geräte so zu sichern, dass die Nutzung durch Unbefugte (zB die eigenen Kinder) verhindert wird? ***Anmerkung:** Generell sollte eine Nutzung durch Dritte unterbunden werden. Weiters sollten die Mitarbeiter in der BYOD-Richtlinie verpflichtet werden, BYOD-Geräte nicht an unsicheren Orten unbeaufsichtigt zu lassen (zB im Auto, am Kaffeehaustisch).*			

Prüffrage	nicht anwendbar	erfüllt	nicht erfüllt
Frage 60: Ist der BYOD-Einsatz in der BYOD-Richtlinie auf mobile Geräte beschränkt, die sich im Eigentum des Mitarbeiters befinden? ***Anmerkung:** Sollte dies nicht der Fall sein und das mobile Gerät zB dem Ehegatten gehören, so wird dessen unbefugter Zugang kaum auszuschließen sein.*			
Frage 61: Wird jeder Mitarbeiter über seine nach dem DSG 2000 und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten belehrt?			
Frage 62: Werden wirksame Zugriffskontrollsysteme für die mobilen Geräte eingesetzt? ***Anmerkung:** In der BYOD-Richtlinie sollten Regeln enthalten sein, längere, nicht zu einfache Passworte und Bildschirmentsperrungen zu verwenden; die Änderungsintervalle sollten festgelegt werden ebenso wie eine kurze Aktivierungszeit für Displaysperren.*			
Frage 63: Ist eine verpflichtende oder automatisierte Installation von Antivirensoftware auf den mobilen Geräten vorgesehen?			
Frage 64: Werden Screenshot-Funktionen bei betrieblichen Datenanwendungen auf den mobilen Geräten unterbunden?			
Frage 65: Werden Cloud-basierte Sprachassistenten (zB Siri) in Geschäftsanwendungen unterdrückt? ***Anmerkung:** Generell sollten Cloud-Dienste für die berufliche Nutzung in der BYOD-Richtlinie unterbunden werden (zB Dropbox, Evernote).*			
Frage 66: Erfolgt der Zugriff auf unternehmensinterne Webportale (zB Intranet) über eigene Browser und wird die Kommunikation zwischen Portal und mobilem Gerät zusätzlich verschlüsselt?			
Frage 67: Wurde eine Fernlöschung und -sperrung eingerichtet, um im Verlustfall die unbefugte Verwendung des mobilen Geräts zu verhindern? Ist in der BYOD-Richtlinie klargestellt, dass und an wen der Mitarbeiter den Verlust/Diebstahl seines Geräts umgehend melden muss und dass er Servicearbeiten nur unter Rücksprache mit der IT-Abteilung durchführen darf?			
Frage 68: Ist in der BV eine unternehmensseitige Protokollierung der tatsächlich durchgeführten Verwendungsvorgänge wie insb Änderungen, Abfragen und Übermittlungen geregelt? Ist dort sichergestellt, dass Mitarbeiter erforderliche (Sicherheits-)Updates durchführen und notwendige Sicherheitseinstellungen vornehmen und dass deren Abänderung/Nichtbefolgung überprüft werden kann?			
Frage 69: Ist bei der Verarbeitung von betrieblichen Daten – abhängig von der Sensibilität dieser Daten – eine ausreichend hohe Frequenz der Synchronisierung mit den Unternehmensservern vorgesehen?			
Frage 70: Ist für die persönlichen Daten des Mitarbeiters ein Backup-Verfahren eingerichtet?			
Frage 71: Sind die Kontroll- und Zugriffsrechte des Unternehmens auf die mobilen Geräte in der BV geregelt?			
Frage 72: Wurde ein Prozess eingerichtet, der im Fall eines Datenmissbrauchs nach Verlust oder Diebstahl eines mobilen Geräts oder sonstiger Verwendung durch Unbefugte die weitere Vorgehensweise in Bezug auf die Informationspflicht des Betroffenen regelt (sog „Data Breach Notification Duty“)?			
Frage 73: Werden die Mitarbeiter entsprechend § 24 DSG 2000 darüber informiert, welche für Daten über sie durch BYOD verarbeitet werden? Werden die Mitarbeiter auf das Datengeheimnis des § 15 DSG 2000 vertraglich verpflichtet? Willigen die Mitarbeiter in IT-forensische Untersuchungen ein? ***Anmerkung:** Diese Punkte können im Rahmen der BYOD-Richtlinie umgesetzt werden, die letzten beiden allerdings nur dann, wenn die BYOD-Richtlinie von jedem Mitarbeiter gegengezeichnet wird.*			
Frage 74: Werden die Mitarbeiter in die Handhabung von BYOD persönlich eingeschult?			
Frage 75: Werden die Mitarbeiter über die Konsequenzen bei Verstößen gegen die BYOD-Regelungen belehrt?			
Frage 76: Wird beim Einsatz von Dienstleistern für BYOD ein Dienstleistervertrag nach §§ 10 und 11 DSG 2000 mit diesen abgeschlossen?			
Frage 77: Wird, soweit erforderlich, vor Beginn von BYOD eine Meldung für durch BYOD zusätzlich anfallende Daten beim Datenverarbeitungsregister eingebracht und, soweit erforderlich, ein Genehmigungsantrag für internationalen Datenverkehr bei der Datenschutzbehörde gestellt?			

Dako 2014/6

Zum Thema

Über den Autor

Prof. KommR Hans-Jürgen Pollirer ist Geschäftsführer der Secur-Data Betriebsberatungs-GmbH. E-Mail: hj.pollirer@secur-data.at

Literatur

WEKA/IT-Management, BYOD – Bring Your Own Device – ein Trend setzt sich mehr und mehr durch (2013) Teil 9/15;

WEKA/Netzwerksicherheit, Bring Your Own Device, Teil 7/12;

Knyrim/Horn, Bring Your Own Device – Ein Trend hält Einzug in Österreichs Unternehmen, ecolex 2013, 365 ff.

Links

- *WKO BSIC*, IT-Sicherheitshandbuch (2014) 20 f, www.wko.at/Content.Node/it-safe/kmu_handbuch_komplett.pdf
- *BITKOM*, Bring Your Own Device, www.bitkom.org/files/documents/20130404_LF_BYOD_2013_v2.pdf
- *Bundesamt für Sicherheit in der Informationstechnik (BSI)*, Überblickspapier Consumerisation und BYOD, www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_BYOD_pdf.pdf?__blob=publicationFile
- *European Network and Information Security Agency (ENISA)*, Consumerization of IT: Top Risks and Opportunities, www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/consumerization-of-it-top-risks-and-opportunities

- *Krampe,* Vereinbarung über die Nutzung von mobilen, privaten Endgeräten für den Zugriff auf die Unternehmensinfrastruktur, www.thomas-krampe.com/byod_vereinbarung.html
- *Deloitte,* Perspektive BYOD Private Hardware in Unternehmen, www2.deloitte.com/content/dam/Deloitte/de/Documents/technology-media-telecommunications/TMT_Report_Perspektive%20BYOD.pdf
- *Franck,* Bring your own device – Rechtliche und tatsächliche Aspekte, RDV 2013, 185 ff, www.gdd.de/downloads/Franck_Aufsatz.pdf