Heißes Eisen nicht nur aus Datenschutz-Sicht: Die Absicherung mobiler Datenträger

Kerstin Blossey, Blossey & Partner

Jeder kennt sie, jeder benutzt sie: mobile Datenträger („mobile devices"). Sie sind aus der digital-globalen Kommunikation nicht mehr wegzudenken und überdies ungemein nützlich und vielfach handlich. Doch je handlicher, desto größer ist die Gefahr, so ein niedliches Teil irgendwo zu vergessen, zu verlieren oder zu verlegen.

In diesem Artikel erfahren Sie...

- Was mobile Datenträger sind und welche gern übersehen werden;
- Welche Anforderungen der Datenschutz an die verarbeitende Stelle hat;
- Was Sie als Nutzer solcher handlichen Geräte sofort tun können.

Was Sie vorher wissen/können sollten...

- Keine spezifischen Vorkenntnisse erforderlich;
- Die Grundbegriffe des Datenschutzes aus den Artikeln der vorherigen Ausgaben sollten geläufig sein. Alternativ kann auf das Glossar von Blossey & Partner (*http://blossey-partner.de/showpage.php?SiteID=11&lang=1*) zurückgegriffen werden.

Peinlich im Privatleben, geschäftsschädigend im Berufsalltag – und darüber hinaus sind alle Stellen, die personenbezogene Daten nicht zu rein privaten Zwecken verarbeiten, verpflichtet, diese mobilen Geräte entsprechend den Maßgaben der geltenden Datenschutzgesetzeslage abzusichern!

Anmerkung in eigener Sache: Dieser Artikel gibt keinen vollständigen Überblick über alle Einzelaspekte, die in der Praxis relevant sein können, sondern greift aufgrund der komplexen Thematik häufige Alltagsfragen auf. Die Inhalte werden zudem nicht juristisch behandelt, sondern ganzheitlich-interdisziplinär betrachtet und dargestellt.

Die Welt der mobilen Datenträger

Unter mobile Datenträger zählen wir grundsätzlich alle Geräte und Arbeitsmittel, die unter eine der folgenden Gruppen einsortiert werden können:

- a) mobile Computer (Laptops, Note- und Netbooks, Tablet-PCs – also alle Geräte, die das Haus verlassen können)
- b) mobile Kommunikationsgeräte (Smartphones, Handhelds, Blackberries, iPhones, Navigationsgeräte, Autotelefone)
- c) mobile Datenspeicher (sämtliche USB-Speichermedien, DVD-ROMs, Bänder, Kassetten etc.)
- d) Sonderfälle mobiler Datenträger (z.B. digitale Kameras, Chipkarten)

Unter die Sonderfälle fallen zum einen mobile Datenträger, auf denen zugleich Daten verarbeitet werden können, die also keine reinen Speichermedien sind. Zum anderen zählen hierzu Datenträger, die in anderen Geräten verborgen sind, zum Beispiel Festplatten für die Zwischenspeicherung zu bearbeitender Daten in Hochleistungskopierern, Faxgeräten und Druckern, Kartenlesegeräte mit Speichereinheiten, digitale Diktiergeräte, Autotelefone (besonders in Leihwägen und Firmenfahrzeugen) und vieles mehr, womit man außerhalb einer festen Installation im Büro und Homeoffice Daten und Informationen bearbeiten kann.

Solche Speichermöglichkeiten werden in der Praxis gern vergessen, weil sie kleine stille Helfer sind, über die man sich für gewöhnlich keine weiteren Gedanken macht.

Datenschutz für mobile Datenträger

Das BDSG stellt einige Datenschutz-Grundprinzipien auf, die der verarbeitenden Stelle dabei helfen sollen, personenbezogene Daten angemessen und wirksam zu erfassen und zu schützen. Diese nachfolgend grob dargestellten Prinzipien gelten auch für die Entwicklung eines geeigneten Schutzniveaus für mobile Datenträger.

Grundsätzlich dreht sich alles bei der automatisierten Verarbeitung personenbezogener Daten um die *Zulässigkeit* der Datenverarbeitung und Nutzung. Die

Einwilligung jedes Betroffenen bzw. seine Benachrichtigung, sofern seine Einwilligung nicht vorliegt bzw. nicht eingeholt werden kann, sollte der normale Weg sein. Gekoppelt damit ist die Datenvermeidung und Datensparsamkeit, nicht zuletzt dabei die Erhebung und Verarbeitung von Informationen ausschließlich zum Geschäftszweck, für den die Daten verarbeitet werden sollen, sofern keine staatlichen bzw. gesetzlichen Interessen vorliegen, die eine solche Verarbeitung sogar erfordern. Das bedeutet, personenbezogene Daten dürfen nicht grundlos und wahllos beschafft und genutzt werden, sondern dies muss zweckgebunden geschehen.

Ein weiteres Grundprinzip – in Verbindung mit Datensparsamkeit ist die geregelte Löschung oder Vernichtung nicht mehr benötigter Daten. Für einige Informationen und Unterlagen (auch digitale Versionen) gelten gesetzliche Aufbewahrungsfristen. So sind beispielsweise E-Mails, die relevante Geschäftskorrespondenz enthalten, nach Handelsgesetzbuch (HGB) aufzubewahren. Hierfür sind zusätzlich Formvorschriften zu beachten, zugleich muss die Wahrung der Privatsphäre der Mitarbeiter sichergestellt sein, wenn die Nutzung des personalisierten geschäftlichen E-Mail-Accounts nicht geregelt oder grundsätzlich erlaubt ist. Ebenso gibt es in vielen Unternehmen einen wahren Wildwuchs von exportierten Datenbeständen, zum Beispiel im vertrieblichen Bereich Exporte aus der Kundendatenbank bzw. dem Customer Relationship Management System (CMS) für die lokale Nutzung außer Haus. Vielfach werden überholte Exportdateien nie gelöscht, sondern einfach neue Dateien hinzugefügt, so dass auch die Rechnersysteme unnötig belastet werden (Speicherbedarf, Indexierung etc.). Die geregelte Löschung, beispielsweise in einem bestimmten Turnus oder eine Vereinbarung, wie lokale Daten von Außendienstmitarbeitern in das zentrale Datensystem einzupflegen und danach die lokalen Daten zu entfernen sind, nützen der Sicherstellung aller Datenschutzziele: der Verfügbarkeit, der Integrität und der Vertraulichkeit der Informationen.

Technische und organisatorische Maßnahmen zum Schutz der Daten auf den Datenträger nach § 9 BDSG sind obligatorisch. Hier sind angemessene Maßnahmen zur Kontrolle des Zutritts, Zugangs und Zugriffs ebenso zu treffen wie zur Weitergabe-, Eingabe-, Verfügbarkeits- und Auftragskontrolle. Das Trennungsgebot soll schließlich die Verarbeitung der personenbezogenen Daten gemäß dem Zweck ihrer Erhebung sicherstellen, zum Beispiel die Trennung der Kundendaten von den Personaldaten.

Die Bereitstellung oder Übermittlung von Daten aus dem oder in das Ausland sowie an über- und zwischenstaatliche Stellen ist ebenfalls datenschutzkonform zu gestalten. Dies spielt für mobile Datenträger unter anderem bei Auslandsreisen eine Rolle, wenn sich die Behörden des Ziellandes vorbehalten, beispielsweise die Laptops bei der Einreise zu überprüfen. Unter Umständen müssen dann sogar verschlüsselte Daten lesbar gemacht werden. Über den Schutz personenbezogener – und gegebenenfalls unternehmenssensibler – Daten muss man sich vor der Einreise Gedanken gemacht haben. Einige Stellen geben ihren Außendienstmitarbeitern inzwischen sogar reine Reiselaptops mit, die jeweils nur mit den Informationen und Datenbeständen ausgerüstet sind, die für diese Reise erforderlich sind. Über geschützte Datenräume werden dann vor Ort weitere Daten nachgeladen oder online verfügbar gemacht. Aber auch bei dieser Methode ist Datenschutz Pflicht: die sorgfältige Auswahl des Anbieters oder auch die Kommunikationsstruktur der Datenübertragungswege müssen geprüft und entsprechend abgesichert sein, um die zu schützenden Daten tatsächlich datenschutzkonform mobil zu behandeln. Auch die Handhabung im Rahmen einer Auftragsdatenverarbeitung muss nach klaren gesetzlichen Regelungen erfolgen.

Insbesondere bei Datenträgern, die nicht nur als reine Speichermedien sondern zur direkten Bearbeitung der Daten dienen, ist § 6c BDSG zu berücksichtigen. Hierunter zählen etwa RFID-Kommunikation, Unternehmensausweise und Chipkarten. Der Gesetzestext sagt Folgendes:

(1) Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, muss den Betroffenen

- 1. über ihre Identität und Anschrift,
- 2. in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten,
- 3. darüber, wie er seine Rechte nach den §§ 19, 20, 34 und 35 ausüben kann, und
- 4. über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen unterrichten, soweit der Betroffene nicht bereits Kenntnis erlangt hat.

(2) Die nach Absatz 1 verpflichtete Stelle hat dafür Sorge zu tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.

! Praxistipp:
Notieren Sie sich ganz bewusst einen Monat lang alle personenbezogenen Daten, die Sie verwenden und notieren Sie sich auch, was sie mit diesen Daten machen (speichern, löschen, verändern, weitergeben, archivieren etc.). Auf diese Weise können sie sich schnell einen realistischen Überblick verschaffen.

(3) Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen, müssen für den Betroffenen eindeutig erkennbar sein.

Für alle relevanten Verfahren gilt auch die *Meldepflicht* nach § 4d f. BDSG. Nur dokumentierte Verfahrensweisen können der Transparenz der Geschäftsprozesse und damit der vom Gesetz angestrebten Wahrung der Recht der Betroffenen dienen.

Nach dem sehr fundierten Ansatz des Grundschutzkataloges des Bundesamtes für Sicherheit in der Informationstechnik (BSI) werden nachfolgende typische *Gefährdungslagen* bei der Nutzung von mobilen Datenträgern unterschieden:

- Von „höherer Gewalt“ wird ausgegangen, wenn ein Datenverlust durch starke Magnetfelder oder etwa durch wechselnde Einsatzumgebung zustande kommt.
- Organisatorische Mängel, wie unzureichende Kenntnis über Regelungen oder Prozesslücken bei der Gewährleistung von fristgerechter Verfügbarkeit.
- Vertraulichkeits-/Integritätsverlust von Daten, die Nichtbeachtung von IT-Sicherheitsmaßnahmen oder gar der sorglose Umgang mit Informationen ist in der Regel auf ein menschliches Fehlverhalten zurückzuführen.
- Technisches Versagen bei defekten Datenträgern oder Verlust beim mobilen Einsatz führt häufig zu Datenverlust.
- Als vorsätzliche Handlungen wird die Manipulation/Zerstörung von IT-Geräten, Zubehör, Daten oder Software betrachtet. Im Weiteren wird Diebstahl, die unberechtigte IT-Nutzung, Computer-Viren, Verbreitung von Schadprogrammen oder Datendiebstahl über mobile Datenträger entsprechend bewertet.

Das Gefahrenpotential bei mobilen Datenträgern ist also vielfältig. Man kann solche Geräte verlegen (unternehmensintern, im Homeofficebereich oder bei dritten Stellen), man sie leicht vergessen (bei Kollegen am Rechner, bei unbefugten Dritten, zu hause), man kann sie verlieren und ermöglichst damit beliebigen Dritten den unbefugten Zugriff, evtl. sogar Weiterverkauf). Die beliebten Geräte können jedoch auch entwendet werden, dahinter steckt in der Regel ein beabsichtigter unbefugter Zugriff, der meist eine sehr zielorientierte Vorbereitung und damit verbunden ein hohes Schadenspotential aufweist, insbesondere ist bei solchen „Pannen“ oft Wirtschaftsspionage anzunehmen. Dies gilt auch für die beabsichtigte oder unbeabsichtigte Manipulation mobiler Datenträger, etwa mit Hilfe von Schadsoftware oder Anwendungen bzw. Techniken zum Ausspionieren der Geräte und Kommunikationsverbindungen (Spyware). Schlussendlich kann es auch zur Zerstörung des Datenträgers kommen, da je nach Art des Geräts unterschiedliche Einflüsse (Magnetismus, mechanische Einwirkung etc.) den Daten gefährlich werden können.

! Praxistipp:
Viele Programme und Geräte bieten von Haus aus die Möglichkeit, eine Unmenge von Daten einzupflegen und zu unterschiedlichsten Zwecken zu verwenden. Hier muss die verarbeitende Stelle klare Regeln aufstellen, welche Daten tatsächlich zu erfassen und nutzen sind. Sind Daten erst einmal im System, ist es vielfach kompliziert oder bedeutet zumindest unnötigen Zusatzaufwand, um sie wieder zu entfernen.

Eingetretene Schadensfälle, in der Regel als Datenschutz-*Pannen* bezeichnet, ziehen konkrete Konsequenzen nach sich. Die Information aller Betroffenen, unter Umständen durch Bekanntmachung in bundesweiten Tageszeitungen (!) ist seit der Novelle II des BDSG, die zum 01.09.2009 in Kraft getreten ist, obligatorisch. Des weiteren entstehen so gut wie immer Kosten und die Bindung weiterer Ressourcen (Personal) zur internen Schadensbegrenzung und Fehlerbehebung. Bußgelder und Haftstrafen (bis zu 300.000 €, das Bußgeld soll seit 01.09.2009 jedoch „den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden“ (§ 43 Absatz 3 Satz 2 f. BDSG). Wie kostenintensiv sich der mit der Panne einhergehende Imageschaden und die weiteren Kosten zur möglichen Rehabilitation in der Gesellschaft und Öffentlichkeit auswirken können, haben die in den vergangenen zwei Jahren in der Presse diskutierten Fälle großer deutscher Konzerne eindrucksvoll verdeutlicht. Der wirtschaftliche bzw. Wettbewerbs-Schaden (z. B. durch Wirtschaftsspionage) lässt sich vielfach gar nicht beziffern, da Innovation in vielen Fällen und unterschiedlichen Entwicklungsstadien kaum messbar ist.

Datenschutz-Maßnahmen für mobile Datenträger

Vorgelagert zu allen Datenschutzmaßnahmen für mobile Datenträger sollte immer ein Konzept für den sicheren Umgang erstellt werden, in welchem die verschiedenen Arten von mobilen Datenträgern, Risiken und Sicherheitsmaßnahmen aufgezeigt werden. Nachfolgend haben wir einige arbeitstaugliche Aspekte zusammengestellt, die jeder umsetzen kann und sollte.

- Jeder kennt gewisse einschlägige Möglichkeiten, mit denen man mobile Datenträger schützen könnte. Einem Laptop kann man vielfach ein Kensington-Schloss verpassen, ein gesetzter Geräte-PIN, der Einsatz eines Dongels sowie eine Grundverschlüsselung des genutzten Mediums kö-

nnen unbefugte Einsichtnahme verhindern. Anwendungspasswörter oder andere Zugriffsschutzmechanismen regeln die Befugnisse der Verarbeitung und Nutzung der Daten. Verschlüsselte Datencontainer entsprechen dem Datentrennungsgebot nach BDSG. Ortungs- und „Selbstzerstörungs"-Dienste, z.B. für Smartphones, sind zwar leider meist kostenpflichtig und mit einer konkreten Ortungsmöglichkeit der Person verknüpft, was Bewegungsprofile ermöglicht. Dafür kann man bei einem Verlust des Geräts zumindest die Daten unbrauchbar machen – wenn man schnell genug ist.

Infrastruktur

In der Praxis kämpfen datenverarbeitende Stellen oft mit der Vielfalt unterschiedlichster mobiler Endgeräte mit verschiedenen Basisausstattungen, was Betriebssysteme, Bedienung und Kompatibilität betrifft. Eine solche Vielfalt ermöglicht zwar ein breites Erfahrungsspektrum bezüglich der Geräte und ihrer Eigenheiten, es erschwert aber zugleich die zentrale Absicherung und Verwaltung solcher Produkte. Dies gilt insbesondere für die unter Punkt 1. c) aufgeführten mobilen Kommunikationsgeräte. Daher raten wir zu einer Konzentration solcher Hilfsmittel auf ein Produkt, das möglichst alle wirklich erforderlichen Anforderungen aus dem Arbeitsalltag erfüllen kann. Die Nutzung eigener (privater) Geräte ist höchstens nach Freigabe durch die IT und (im Zweifelsfall) in Rücksprache mit dem DSB zu gestatten, besser wäre jedoch eine saubere Trennung geschäftlicher und privater Infrastruktur, um die Datentrennung nach § 9 BDSB (Anlage) gewährleisten zu können. Jedes fremde Gerät erhöht die Vielzahl unterschiedlicher Geräte und damit den Verwaltungsaufwand für das Unternehmen!

Oft stellt sich bei einer ernsthaften Auseinandersetzung mit den *Features* und Anwendungen eines solchen Geräts heraus, dass auf manche Anforderung gut verzichtet werden kann – auch in der *Chefetage*. Einheitliche Geräte für alle (ohne Ausnahmen!) fördern Überblick (Inventarisierung), die Auswahl und fachgerechte Realisierung von geeigneten Schutzmaßnahmen und die Kontrolle der Wirksamkeit getroffener Maßnahmen. Zugleich erleichtern sie auch die Überwachung der ordnungsgemäßen Nutzung durch den jeweils zugeordneten Beschäftigten, etwa die private Verwendung des geschäftlichen E-Mail-Accounts oder das Teilen personenbezogener User-Accounts.

Um eine geregelte Inventarisierung gewährleisten zu können, die auch die gesetzlich vorgeschriebene Transparenz zur Wahrung der Betroffenenrechte berücksichtigt, müssen alle verwendeten Geräte nach Geräteart, Typ, Hersteller, Version, Benutzer und Sicherheitsmaßnahmen lückenlos aufgelistet werden. Die Zuordnung zwischen inventarisiertem Produkt und dem zugeteilten Benutzer erleichtert neben der wirtschaftlichen Verlustabsicherung die Kontrolle, dass keine Unternehmensdaten (insbesondere keine personenbezogenen Informationen) durch Unbefugte (ausgeschiedener Mitarbeiter, dem das Gerät zugeordnet wurde, der es nach seinem Ausscheiden aber nicht zurückgegeben hat) auf den freien Markt gelangen können. Nur durch eine entsprechende schriftliche Dokumentation kann die IT-Administration in diesem Fall Regelung der Geräteausgabe und Rückgabe für die Beschäftigten nachweisen und daher disziplinarische Maßnahmen gegen sich selbst vermeiden.

Grundsätzliche Schutzmaßnahmen

- Zu den grundsätzlichen Schutzmaßnahmen zählt, dass der Beschäftigte sich darüber bewusst sein muss, dass er ein leicht einsehbares und leicht verlierbares Gerät mit Unternehmens- und personenbezogenen Daten erhält, für das er – samt Inhalten – solange die Verantwortung trägt, wie das Gerät in seinem Besitz ist;
- Auch der Sichtschutz ist eine grundsätzliche Schutzmaßnahme. Einige Anbieter haben z.B. Folien entwickelt, die vor den Monitor gespannt werden können und die dann jegliche Einsichtnahme, die nicht direkt durch den davor Sitzenden erfolgt, unmöglich macht. Dies ist eine wichtige und einfache Maßnahme sowohl im Bereich des Kundenservice als auch für das digitale Arbeiten unterwegs (ein Hersteller ist z.B. 3M);
- Die Geräte-PIN (zum Beispiel bei Mobiltelefon), Funktions-PIN (zum Beispiel bei Telefonfuntionen, Bluetooth oder WLAN) oder ein Geräte-Dongel bieten entsprechende Einschränkungen bei Nutzerberechtigungen;
- Der Personenbezogene Login und ein sicheres Passwort sind eine wirksame Barriere, um die grundsätzliche Nutzung des Geräts zu verhindern, sofern ein Zugriff auf sensible Daten möglich wäre (temporäre Dateien, Anruflisten, E-Mail-Postfächer etc.);
- Bei der Remote-Löschfunktion bieten inzwischen viele Kommunikationsmedien Möglichkeiten an, die Geräte registrieren zu lassen und so bei Verlust ein Löschen der Daten oder ähnliches zu ermöglichen, möglichst bevor unbefugte Dritte Zugriff nehmen können;
- Arbeitsrechtliche Regelungen können den Beschäftigten klare Vorgaben liefern, wo er Verantwortung zu tragen hat und was er bei Verlust eines Gerätes

! Praxistipp:
Bitte vergewissern Sie sich vorher, dass es nicht bereits Regelungen und Verfahrensanweisungen in Ihrem Unternehmen dazu gibt, damit Sie eventuell bestehende Maßnahmen nicht außer Gefecht setzen!

zu tun hat. Darüber hinaus kann er dazu verpflichtet werden, eine entsprechende Verlustmeldung zu tätigen. Ferner informieren diese Regelungen den Beschäftigten darüber, welche Sanktionen bei Nichtbeachtung geltend gemacht werden können. Regelungen dieser Art müssen ausnahmslos für alle Hierarchieebenen und Nutzer solcher Geräte im Unternehmen gelten. Führungspersonal hat hier Vorbildfunktion;

Schutz der enthaltenen Inhalte

- Durch die Verschlüsselung des kompletten Geräts kann der Zugriff auf sämtliche, auch in Systemdateien oder temporär vorgehaltene Daten ausgeschlossen werden. Dies gilt sogar bei einer Verwendung von so genannten Live-CDs, die z.B. mit einem mobilen Linuxsystem Windowspasswörter nutzlos machen und so vielfach Vollzugriff auf alle Inhalte bieten;
- Nach BDSG dürfen keine personenbezogenen Daten verarbeitet werden, die nicht benötigt werden! Datensparsamkeit ist hier gefordert. Außerdem schont diese Überlegung gerade bei mobilen Telefonen die Speicherkapazität und nicht zuletzt damit die Performance;
- Die Ablage aller Inhalte in verschlüsselten Partitionen bietet den Benutzern eine einfache und effiziente Schutzmaßnahme. Es gibt jede Menge Programme (OpenSource ebenso wie propreritäre), die eine Ablage in solchen „Datencontainern“ ohne große Mühe für den Benutzer erlauben. Das Programm startet automatisch mit der Betriebsbereitschaft des Gerätes. Die Eingabe eines wirksamen Passwortes reicht dann in der Regel aus, um den Container zu öffnen. Die meisten Programme bieten die Nutzung mehrere solcher Container getrennt voneinander, so dass z.B. für unterschiedliche Kunden oder Geschäftszwecke die Daten sauber getrennt aufbewahrt werden können;
- Personenbezogene Daten, die zu unterschiedlichen Zwecken verarbeitet werden, z.B. Personal- und Kundendaten, sollten getrennt aufbewahrt werden. Dies gilt auch für die Daten unterschiedlicher Kunden, wenn deren Datenbestand sensibel ist oder entsprechende Verschwiegenheitsvereinbarungen (NDA's) getroffen wurden;
- Auch die Verschlüsselung von E-Mails ist inzwischen leicht und unkompliziert mit einem entsprechenden Programm lösbar. Benötigt werden in der Regel ein Schlüsselpaar, wobei der private Key möglichst vertraulich angelegt und aufbewahrt werden muss, und eine Passphrase (längeres Passwort). Der Vorteil eines solchen Programms ist, das E-Mails damit nicht nur verschlüsselt, sondern auch einfach nur digital unterschrieben (signiert) werden können, wodurch die Authentizität des Absenders und die Integrität des gesendeten Inhalts sichergestellt werden können;
- Ferner sollten auch Viren- und Trojanerscans für mobile Kleingeräte obligatorisch sein. Zusätzlich kann eine Regelung im Umgang mit Daten unbekannter Absender das Risiko einer Infizierung vermindern;
- Personenbezogene Daten müssen anonymisiert (oder wenigstens pseudonymisiert) verarbeitet und gespeichert werden, soweit das möglich ist. So ist es nützlich, Kunden generell ein Kürzel zu geben, statt ihren Klartextnamen zu verwenden, wenn nicht unbedingt jeder wissen soll, welche Kunden das Unternehmen betreut. Dasselbe gilt für Personaldaten: Einsatzpläne benötigen in den seltensten Fällen die vollen Namen und die Personalnummer. Meist genügt die Personalnummer oder gar eine völlig gesonderte Nummer. Bei Personen sollte man auf Initialen und andere geeignete Kürzel zurückgreifen. Dies gilt insbesondere für Protokolle und ähnliches, wo volle Namen nicht erforderlich sind.

! Praxistipp:
Damit Ihnen der Anfang leichter fällt, haben wir die wichtigsten Aspekte aus diesem Artikel in einer Checkliste zusammengestellt. Diese erhalten Sie unter *http://blossey-partner.de/showpage.php?SiteID=6&lang=1*. Auf dieser Seite bitten wir Sie (freiwillig und ohne Registrierung) um ein paar Angaben zu Ihnen als Leser/Interessent: Ihre Altersgruppe, Beruf, Position, Bundesland; über diese Infos würden wir uns sehr freuen, um uns einmal einen groben Überblick über unsere Leser verschaffen zu können. Wenn Sie keine Daten angeben möchten, kreuzen Sie einfach die entsprechende Option an. Herzlichen Dank im Voraus!

Sensibilisierung der Beschäftigten

Sowohl Behörden als auch Unternehmen setzen zunehmend unterschiedlichste Arten mobiler Datenträger ein. Dies sind oftmals auch Geräte, die in ihrer ersten Einschätzung keine offensichtliche Funktion als mobiler Datenträger aufweisen. Dadurch steigt sowohl die Zahl der Verbreitungswege für Informationen als auch die Zahl möglicher Sicherheitslücken. Zwar können einige dieser Sicherheitslücken technisch minimiert werden, aber ohne die Einbeziehung verantwortungsbewusster Mitarbeiter in den sicheren und sachgerechten Umgang mit mobilen Datenträgern kann diesem Umstand kaum zielführend gerecht werden.

Spätestens bei Übergabe an den Mitarbeiter ist dieser möglichst vollumfänglich über die Art und die Einsatzmöglichkeiten seines mobilen Datenträgers aufzuklären und auf den sorgsamen Umgang zu verpflichten. Dies schließt Informationen über die Bauform, die Gerätevariante, sämtliche Nutzungsmöglichkeiten und deren potentielle Risiken und Probleme bei Fehlnutzung ein. Zudem sollte der Beschäftigte insbesondere über

Aktueller Rückblick zu den Datenschutz-Schlagzeilen in der Online-Presse:

Das Redaktionsteam von Blossey & Partner stellt jede Woche neu die Schwerpunktthemen rund um die heißen Datenschutzthemen für Sie zusammen unter http://www.blossey-partner.de (*News*, unten rechts). Klicken Sie doch mal hinein, das Archiv reicht inzwischen bis 2005 zurück und bietet sogar eine Suchfunktion. Viel Spaß beim Stöbern.

die Grenzen der unternehmensseitig eingesetzten Sicherheitsmaßnahmen aufgeklärt werden. Neu erkannte Gefahrenpotentiale und Aspekte zur Nutzung der mobilen Datenträger und Geräte können dem Mitarbeiter fortlaufend, z.B. durch entsprechende Artikel im Intranet des Unternehmens, zugänglich gemacht werden.

Arbeitsanweisungen oder Betriebsvereinbarungen regeln den richtigen Umgang mit mobilen Datenträgern und Geräten, deren richtige Führung und Aufbewahrung und beugen damit einem Verlustfall vor. Weiterführend wird dabei das richtige Verhalten bei Verlust des Gerätes erläutert, sowie eine entsprechende Darstellung der Konsequenzen bei Zuwiderhandlungen aufgeführt. Es empfiehlt sich zudem die Art der Daten, die auf dem mobilen Datenträger gespeichert werden dürfen zu definieren. Insbesondere ein wirksamer Schutz vor unbefugtem Zugriff, Manipulation oder Datenverlust, z. B. durch Geräte-PIN, ist hier anzuweisen.

Bei Rückgabe/Wechsel des Gerätes ist sicherzustellen, dass alle personenbezogenen und unternehmenssensiblen Daten wirksam, das heißt nicht mit normalem Aufwand wiederherstellbar, gelöscht werden.

Fazit

Ein angemessener Schutz mobiler Datenträger ist auch mit einfachen Mitteln schnell zu erreichen. Entscheidend ist neben all den genannten Aspekten, dass die Benutzer den Sinn realisierter Maßnahmen nachvollziehen können und sich bewusst sind, dass Pannen aufgrund der mangelnden Compliance des Beschäftigten Konsequenzen hat.

KERSTIN BLOSSEY, BLOSSEY & PARTNER

Der Autorin ist Dipl. Sozialpädagogin (FH), Dipl. Informations-Wirtin (FH) und Gründerin von Blossey & Partner, einem kleinen Unternehmensberatungshaus, das sich ganz auf den unternehmerischen Datenschutz spezialisiert hat. Zum Kundenkreis zählen deutsche wie international angesiedelte mittelständische Unternehmen, Konzerne und Einrichtungen des öffentlichen Dienstes aus so unterschiedlichen Branchen wie Druck & Medien, IT- Anwendungen & IT-Sicherheit, Telekommunikation, Verlagswesen, Softwareindustrie, Automotive, Gesundheitswesen, Forschung, Tourismus, produzierendes Gewerbe und die öffentliche Hand. In gelegentlichen Fachbeiträgen und Vorträgen vermittelt die Autorin schwerpunktmäßig wirtschaftlich angemessene und arbeitstaugliche Möglichkeiten und Wege des praxisorientierten Datenschutzes.