INHALT

Schwerpunktthema auf den Seiten 5 bis 13:

Totalkontrolle im Namen der Informationssicherheit?

Datensicherheit versus Datenschutz am Beispiel des Einsatzes der Kassen-Software „LossPrevention" ..... **Seite 5**

Informationsschutz durch Data Loss Prevention – Hintergründe, Wissenswertes, Tipps, Fallbeispiele ..... **Seite 10**

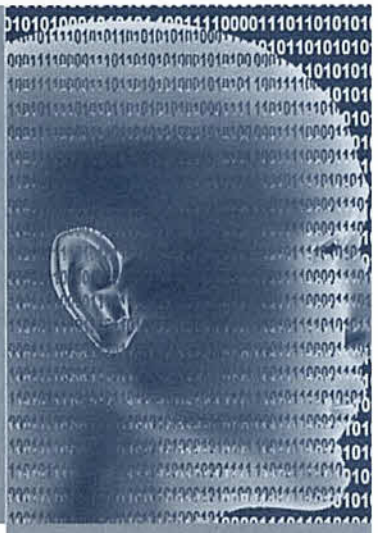


Foto: Baum Rete

Mini-Braillezeilen

Blinde und Sehbehinderte können jetzt auch im mobilen (Arbeits-)Leben von immer kleinerer und immer leistungsfähigerer Technik profitieren ..... **Seite 19**

Foto: E. Novation BT

Mobile Ortung

Möglichkeiten zur Ortung und damit zur Überwachung von Mitarbeitern sind mittlerweile reichlich vorhanden. Klare Regelungen sind daher dringend nötig ..... **Seite 26**

SCHWERPUNKT: TOTALKONTROLLE IM NAMEN DER INFORMATIONSSICHERHEIT?

Datensicherheit versus Datenschutz

am Beispiel des Einsatzes der Kassen-Software „LossPrevention“

Jan A. Strunk // Rechtsanwalt, Fachanwalt für IT-Recht und für Arbeitsrecht, Kiel

HIER LESEN SIE:

- die umfangreichen technischen Überwachungs- und Auswertungsmöglichkeiten mit einem sogenannten Data-Loss-Prevention-Tool
- die mitbestimmungs- und datenschutzrechtlichen Rahmenbedingungen für den Einsatz von Programmen zum Informationsschutz
- den einzig praktikablen Weg für Belegschaftsvertretungen, um die Mitarbeiter vor einer Totalkontrolle durch diese Art von Software zu bewahren

In Zeiten wie diesen, in denen Informationen – und vor allem die Herrschaft über sie! – zum wertvollsten Gut eines Unternehmens gehören, rücken die Kernthemen der Verantwortlichen für die Informationssicherheit verstärkt in den Fokus der öffentlichen Wahrnehmung. Die öffentlich gewordenen Datenlecks bei großen Konzernen (nicht nur) der Unterhaltungselektronik, bei Banken und Behörden sowie in sozialen Netzwerken sind hierfür aktuelle Beispiele. Vorbeugende Schutzmaßnahmen stehen daher hoch im Kurs. Das in diesen Fällen auch unter dem Begriff „Data Loss Prevention“ bekannte Vorgehen greift jedoch massiv in die Rechte der Beschäftigten ein und schießt oft über das eigentliche Ziel hinaus. Eine Totalkontrolle ist mit diesen Tools problemlos möglich, wie dieser Schwerpunkt zeigt – wenn die Belegschaftsvertretung nicht rechtzeitig klare Grenzen zieht.

Betrieblichen Maßnahmen zur Datensicherheit und zum Datenschutz wird in der Folge dieser neueren Entwicklung – wenn auch zum Teil ersichtlich erst unter dem Eindruck bereits bekannt gewordener eigener Versäumnisse – aufgrund der potenziell schwerwiegenden Folgen, die etwa ein ungewollter und unkontrollierbarer Informationsabfluss für den geschäftlichen Erfolg und das Kundenvertrauen haben kann, auch unternehmensintern inzwischen erkennbar häufiger die gebührende Priorität eingeräumt.[1]

Für die begriffliche Funktions-Kennzeichnung entsprechender betrieblicher Präventivmaßnahmen – die sowohl als Software als auch als Hardware von den Herstellern entsprechende IT-Sicherheitslösungen angeboten werden – ist mittlerweile der englische Begriff „Data Loss Prevention“ (auch in der Abkürzung „DLP“) verbreitet.

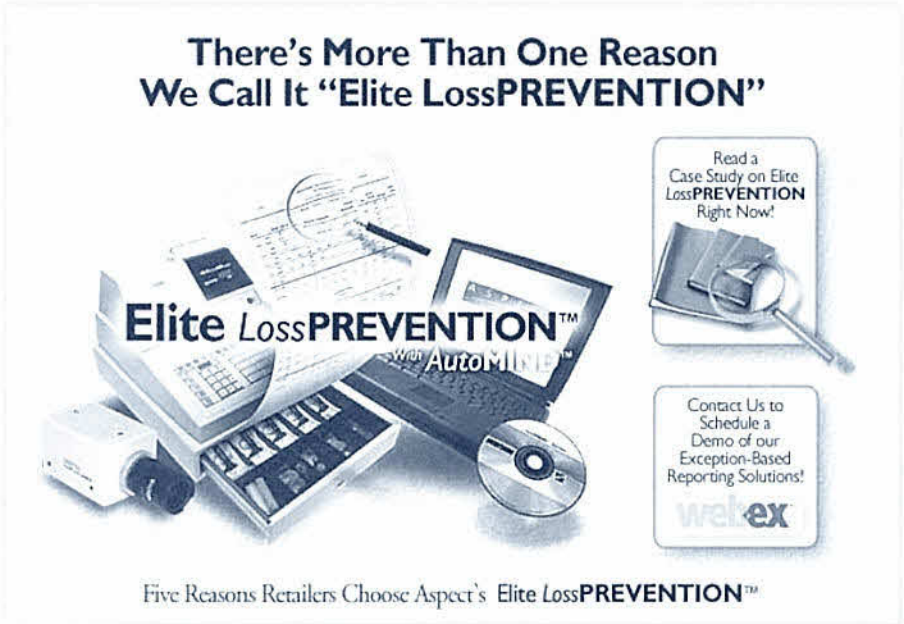
Nun liegt es allerdings bei der Ein- und Durchführung geeigneter Maßnahmen zum Schutz von Informationen im Arbeitsverhältnis in der Natur der Sache, dass diese fast ausnahmslos mit Beschränkungen und Kontrollen verbunden sind, die den Beschäftigten auferlegt werden.

Hierbei wird man sicherlich eine ganze Reihe von Absicherungen benennen können, deren Sinn sich auch dem Laien ohne Weiteres erschließt und die für einen ver-

ständigen Mitarbeiter objektiv nachvollziehbar und akzeptabel sind. So wird etwa niemand ernsthaft ein Problem damit haben, wenn ein Computer am Arbeitsplatz den Anschluss externer Datenträger nicht zulässt, wenn diese Funktion für dienstliche Zwecke nicht benötigt wird oder wenn die PC-Nutzung nur unter Verwendung einer gültigen, regelmäßig wechselnden Zugangskennung möglich ist.

Aber in vielen Fällen geht es tatsächlich weniger um Datenschutz als um Datensicherheit zugleich auch dem Schutz des einzelnen Mitarbeiters dienen (z. B. ermöglicht ein durch geheimes (!) Passwort geschützter PC-Zugang eine korrekte Zuordnung der Verantwortung für erfolgte Bedienereingriffe). Meist aber dienen sie ausschließlich dem – grundsätzlich durchaus berechtigten – Interesse des Unternehmens an der Herrschaft über „seine" Daten.

DLP-Maßnahmen sind daher stets nicht nur daran zu messen, ob sie dem Unternehmen objektiv einen Zuwachs an (Daten-)Si-



Im Einzelhandel wird zur Aufdeckung von Kassenfehlbeständen auch die Software „Loss Prevention" eingesetzt, die riesige Datenmengen in kurzer Zeit auswerten kann …

tensicherheit. Die Begriffe sind in ihrer Bedeutung nicht synonym und soweit es den Datenschutz betrifft, wird diese auch gelegentlich verkannt. Denn obwohl der Wortsinn des Begriffs „Datenschutz" es vordergründig nahelegen mag:

Geschützt werden durch ihn nicht die Daten, sondern stets der Mensch, der mit ihnen in einem persönlichen Zusammenhang steht.

Der Zweck des Datenschutzes besteht darin, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt wird.

Die Maßnahmen, die begrifflich unter dem Schlagwort DLP versammelt werden, haben dagegen nicht zwingend diese Zielsetzung: Zwar kann eine Maßnahme zur cherheit bringen, sondern vor allem auch danach zu beurteilen, ob sie die Persönlichkeitsrechte der Mitarbeiter hinreichend respektieren und ihnen daher in Übereinstimmung mit den (datenschutz-)rechtlichen Anforderungen zugemutet werden dürfen.

Besonders deutlich wird das bei solchen Maßnahmen, bei denen es vorrangig weniger darum geht, unternehmensrelevante Informationen vor der unbefugten Weitergabe an Dritte zu schützen (also den Verlust von Daten zu verhindern), sondern die Zielrichtung von vornherein zumindest auch die – direkte oder indirekte – Gewinnung von Informationen über das Verhalten der Beschäftigten (also die Datenerhebung) ist, um Schädigungen des Unternehmens zu verhindern oder jedenfalls aufzudecken.

Anhand eines konkreten Beispiels will dieser Beitrag einmal die grundsätzlichen datenschutz- und mitbestimmungsrechtlichen Rahmenbedingungen für den Einsatz von DLP-Tools im Überblick skizzieren.[2]

Rahmenbedingungen für den Einsatz von DLP-Software

Im deutschen Einzelhandel wird von großen Filial-Unternehmen seit Jahren zur Aufdeckung von Kassenfehlbeständen, die durch fehlerhafte Bedienung oder aber durch Manipulationen der Kassenbedienung entstehen, unter anderem die Software „LossPrevention" eingesetzt.[3]

Wesentliches arbeitgeberseitiges Ziel der Nutzung ist die Entdeckung und Reduzierung von Vermögensverlusten aus Manipulationen bei Kassentransaktionen, sowie das Erkennen von Schwachstellen in der Bedienung der eingesetzten Hard- und Software und im Umgang mit organisatorischen Regelungen im Kassenbereich.

Der Hersteller der Software selbst beschreibt die Fähigkeiten und Vorzüge seines Produkts so:

> „LossPrevention bietet die Möglichkeit, riesige Datenmengen innerhalb kurzer Zeit auszuwerten, um zentralseitig Manipulationen in der Filiale aufzudecken und zu verfolgen. Dazu greift LossPrevention auf alle in den Filialen gesammelten Daten zurück. Eine außergewöhnlich hohe Anzahl von Stornierungen, häufige Leergutauszahlungen, mehrere Kartentransaktionen mit derselben manuell eingegebenen Kreditkartennummer – das System kennt die vielfältigen Betrugsmöglichkeiten, zeigt Ihnen Auffälligkeiten auf und liefert Ihnen die dringend benötigten Beweise. LossPrevention liefert grafische und tabellarische Darstellungen und ermöglicht dem Benutzer, unregelmäßige Transaktionen an der Kasse schnell zu erkennen und zu verfolgen. Ausgewählte Informationen können auf Wunsch weiter detailliert werden. Neben den verfügbaren Standard- und kundenspezifischen Berichten, können bei Bedarf zusätzliche Berichte definiert werden." [4]

Die Software LossPrevention ist aus Unternehmersicht auch deshalb so interessant und mit Blick auf ihr Verwendungspotenzial so reizvoll, weil sie zentral auf die Originaldaten sämtlicher Kassenvorgänge der an das Unternehmensnetzwerk angeschlossenen Kassenterminals aller konzernzugehörigen Filialen zugreifen und diese nach beliebigen Kriterien und Zielsetzungen auswerten, analysieren und bei Bedarf bis zum jeweiligen Filial-Kassenterminal zurückverfolgen kann (sogenanntes „Data-Mining").[5]

Das zur Verfügung stehende Datenmaterial ist also sehr umfangreich und daher recht aussagekräftig.

Es bedarf vor diesem Hintergrund nicht allzu großer Phantasie, um das Spannungspotenzial zu erahnen, das sich aus derart mächtigen automatisierten und administrierbaren Fähigkeiten einerseits und andererseits dem bereits erwähnten Grundrecht auf informationelle Selbstbestimmung der Beschäftigten eröffnet.

Und es stellt sich die ganz praktische Frage, unter welchen rechtlichen Voraussetzungen die Durchführung einer so weitreichenden Datenverarbeitung im Unternehmen zulässig ist. Ihr wollen wir nun näher nachgehen.

Zulässigkeit von Datenverarbeitungen

Soweit es Datenverarbeitungen im Arbeitsverhältnis betrifft, kommen als zu beachtende Rechtsvorschriften thematisch in erster Linie die Regelungen des Bundesdatenschutzgesetzes (BDSG) sowie des Betriebsverfassungsgesetzes (BetrVG) in Betracht. Daneben können arbeitsrechtliche Bestimmungen eine Rolle spielen, vor allem Betriebsvereinbarungen.

Das BDSG hat die Verarbeitung von personenbezogenen Daten juristisch ausgedrückt als sogenanntes Verbot mit Erlaubnisvorbehalt ausgestaltet. Übersetzt bedeutet das: Es ist grundsätzlich verboten, es sei denn, irgendwo steht, dass es doch erlaubt ist. Dieser Gedanke ist in § 4 Abs. 1 BDSG ausformuliert. Der ordnet an, dass eine Verwendung personenbezogener Daten nur zulässig ist, soweit es das BDSG oder eine andere Rechtsvorschrift erlaubt oder der Betroffene in die konkrete Datenverwendung wirksam eingewilligt hat.

Der Aspekt der Einwilligung, also einer freiwilligen Akzeptanz durch die Arbeitnehmer spielt bei der hier zu betrachtenden DLP-Maßnahme keine ernsthafte Rolle. Es ist in der arbeitsrechtlichen Diskussion schon grundsätzlich umstritten, ob es die vom Gesetz gemeinte Freiwilligkeit innerhalb eines abhängigen Beschäftigungsverhältnisses überhaupt gibt.[6] Jedenfalls aber ist die Nutzung der Revisions-Software faktisch unabdingbar für den Einsatz eines Mitarbeiters an der Kasse. Wer hierzu sein Einverständnis nicht erklärt, kann den Job nicht machen. Hier scheidet bezüglich der abverlangten Entscheidung über die Datenpreisgabe jede echte Entschließungsfreiheit aus.

Eine Rechtfertigung für die fragliche Datenverarbeitung kann sich hier daher nur aus geschriebenem Recht ergeben.

Gesetzliche Rechtfertigung

Soweit es LossPrevention betrifft, käme als einschlägige gesetzliche Erlaubnisnorm nur § 32 Abs. 1 BDSG in Betracht.

Nach Satz 1 dieser Vorschrift, die seit September 2009 gilt, dürfen personenbezogene Daten eines Beschäftigten dann erhoben, verarbeitet oder genutzt werden, wenn dies im Rahmen der verschiedenen Phasen eines Arbeitsverhältnisses, das heißt seiner Begründung, Durchführung oder Beendigung erforderlich ist.

Personenbezogene Daten sind gemäß § 3 Abs. 1 BDSG „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person". Da LossPrevention über die Funktionalität verfügt, dass sich über die Kassenidentität bzw. die Bedienernummer die jeweiligen Mitarbeiter ohne großen Ermittlungsaufwand ausfindig machen lassen – also bestimmbar sind, ist diese Voraussetzung unproblematisch erfüllt.

Das wirft die weitere Überlegung auf, ob die fraglichen Kassendaten „zur Durchführung" des Arbeitsverhältnisses „erforderlich" sind.

Zur Durchführung des Arbeitsverhältnisses bestimmt sind die Daten, die der Arbeitgeber zur Erfüllung seiner Pflichten, aber auch zur Wahrnehmung seiner Rechte gegenüber dem Arbeitnehmer vernünftigerweise benötigt.[7] Das wird man ganz allgemein für die fraglichen Daten der Kassenvorgänge zunächst bejahen können.

Erlaubt sind nach dem Willen des Gesetzgebers jedoch nur solche Verarbeitungen, die für das Arbeitsverhältnis als geboten und nicht nur als „nützlich" zu bewerten sind.[8] In der Sache geht es dabei um einen angemessenen Ausgleich zwischen den Eigentumsrechten des Arbeitgebers (darauf beruht letztlich die Anerkennung seines Kontrollinteresses) und den Persönlichkeitsrechten der Arbeitnehmer. Beiden Rechtspositionen kommt verfassungsrechtlicher Schutz zu, so dass hier ein sachgerechter Ausgleich der beiderseitigen Interessen erfolgen muss.

„Die Data-Mining-Fähigkeiten der Software ermöglichen insbesondere die nahezu unbegrenzte Verknüpfung einzelner Daten zu beliebigen Auswertungszwecken."

Nun wird man das eingangs beschriebene Ziel des Arbeitgebers, einem Fehlverhalten seiner Arbeitnehmer – sei dieses nun vorsätzlich mit dem Ziel einer Schädigung oder lediglich fahrlässig aufgrund mangelhafter Sachkunde erfolgt – entgegenzuwirken, sicherlich als zweckmäßig bzw. notwendig und die zu seiner Verwirklichung dienende Maßnahme somit grundsätzlich als „erforderlich" im Rechtssinne bewerten können. Kontrollen, ob der Arbeitnehmer seinen aus dem Arbeitsvertrag geschuldeten Pflichten nachkommt, gelten ebenfalls als erforderlich zur Durchführung des Arbeitsverhältnisses. Hierunter fallen auch präventive Kontrollmaßnahmen, die bewirken sollen, dass Pflichtverletzungen erst gar nicht stattfinden.[9]

Allerdings vollzieht sich durch LossPrevention nicht nur eine durchgängige und lückenlose Kontrolle sämtlicher Kassenbedienungsvorgänge und in der Folge auch der Systemzugriffe jedes einzelnen Bedieners. Die Data-Mining-Fähigkeiten

der Software ermöglichen insbesondere die nahezu unbegrenzte Verknüpfung einzelner Daten zu beliebigen Auswertungszwecken. Hierdurch können für den Arbeitgeber neben den reinen kassenbezogenen Kontrollen noch ganz andere, höchst interessante Details bezüglich des Arbeitsverhaltens erkennbar werden: Etwa das Bedienungstempo (Abwicklung der Kassenvorgänge) oder auch die Einhaltung von Arbeitspausen. Damit verschiebt sich die Zielrichtung einer Maßnahme zum Vermögensschutz deutlich zu anderen potenziellen Zwecken, insbesondere dem der Leistungskontrolle.

Und es kommt hinzu, dass die Überwachung durch LossPrevention – anders als etwa bei einer offenen Videoüberwachung – nicht direkt wahrnehmbar und vom Arbeitnehmer in ihrem ganzen Ausmaß überschau- bzw. einschätzbar erfolgt.

Schließlich erlaubt das vollständige „Funktionsarsenal" der Software eine Überwachungstiefe, die deutlich über das hinausgeht, was zur bloßen Diebstahlsprävention oder Feststellung von Schulungsbedarf notwendig wäre.

Durch LossPrevention kommt es zwar nicht gleich zur vollständigen Erstellung eines Persönlichkeitsprofils, jedoch befähigt die Nutzung den Arbeitgeber regelmäßig zur Erstellung eines umfassenden, den bereits genannten Zweck klar überschreitenden Nutzungsprofils.

Ein derart intensiver Eingriff in das Persönlichkeitsrecht der Mitarbeiter ist zur Wahrung der schützenswerten arbeitgeberseitigen Interessen, die im Zusammenhang mit dem Beschäftigungsverhältnis der mit der Kasse betrauten Mitarbeiter (also zur Durchführung des entsprechenden Arbeitsverhältnisses) bestehen mögen, daher offensichtlich nicht erforderlich. Er ist deshalb als unverhältnismäßig und somit rechtlich unzulässig zu bewerten.

Mit Satz 2 des § 32 Abs. 1 BDSG existiert allerdings noch ein weiterer gesetzlicher Rechtfertigungstatbestand, der inhaltlich zum Tragen kommen könnte:

Nach dieser Vorschrift dürfen personenbezogene Daten eines Beschäftigten zur Aufdeckung einer Straftat dann verarbeitet werden, wenn tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat und „das schutzwürdige Interesse des Beschäftigten an einem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt".

Mit Blick auf den generellen und systematischen unternehmensweiten Einsatz von LossPrevention sind jedoch schon zwei Punkte tatbestandlich problematisch:

Zum einen liegt dem Einsatz der Software im Normalfall kein konkreter Anlass zugrunde. Grund für die Einführung ist vielmehr die allgemeine Erfahrung bzw. das Wissen des Arbeitgebers, dass Mitarbeiterdiebstähle immer stattfinden. Der Erlaubnistatbestand setzt aber ein anlassbezogenes Vorgehen voraus. Er ist lediglich zur Rechtfertigung solcher Maßnahmen gedacht, die den Arbeitgeber in die Lage versetzen sollen, einem konkreten Tatverdacht zielgerichtet nachzugehen.[10]

Und zum anderen dürfen sich etwaige Kontrollmaßnahmen dann auch nur gegen einen konkret Verdächtigen richten. LossPrevention funktioniert aber vor allem deshalb so gut, weil es unterschiedslos alle Kassenvorgänge und damit alle Kassenbediener unabhängig von irgendeinem konkreten Tatverdacht kontrolliert und damit systembedingt erst einmal alle Kassenmitarbeiter faktisch unter „Generalverdacht" stellt. Darin jedoch liegt keine zielgerichtete Maßnahme gegen einen konkreten Betroffenen. Bereits an dieser Stelle scheitert also die Rechtfertigung aus dem Gesetzestatbestand.

Unabhängig davon wäre auch die weitere Voraussetzung des § 32 Abs. 1 Satz 2 BDSG nicht erfüllt:

Da der bei der Interessenabwägung zu berücksichtigende Eingriff in das Persönlichkeitsrecht der Beschäftigten sowohl wegen des Umfangs der Datenerhebung als auch wegen der systematischen Einbeziehung völlig unverdächtiger Personen (die nämlich im Ergebnis Gefahr laufen, sich bei Nutzung von LossPrevention ohne Not einer etwaigen Verdachtssituation auszusetzen) mit Blick auf das schützenswerte Kontrollinteresse des Arbeitgebers deutlich zu schwer wiegt und sich auch aus den bereits zu Satz 1 der Vorschrift angesprochen Gründen als unverhältnismäßig darstellt, würde man den schutzwürdigen Interessen der Arbeitnehmer hier in jedem Fall den Vorzug zu geben haben und die Zulässigkeit der Datenverarbeitung durch LossPrevention auch hieran scheitern lassen müssen.

Regelung durch Betriebsvereinbarung

Zu Beginn des Beitrags ist der Grundsatz vorgestellt worden, dass eine Datenverarbeitung gemäß § 4 Abs. 1 BDSG dann zulässig ist, wenn das BDSG oder eine andere Rechtsvorschrift dies erlaubt. Als Rechtsnorm in diesem Sinne gelten anerkanntermaßen auch Betriebs- und Dienstvereinbarungen.[11] Auch auf sie kann also die Zulässigkeit einer personenbezogenen Datenerhebung und -auswertung gestützt werden.

Betriebsverfassungsrechtliche Mitbestimmungstatbestände, durch die die Zustimmung des Betriebsrats zur Rechtmäßigkeitsvoraussetzung wird, ergeben sich beim Einsatz von LossPrevention unter dem Aspekt der formalisierten Erhebung von Personaldaten (§ 94 BetrVG), datenschutzrelevanter Regelungen im Bereich der betrieblichen Ordnung und des Verhaltens (§ 81 Abs. 1 Nr. 1 BetrVG) und last but not least wegen der Einführung bzw. des Einsatzes technischer Überwachungseinrichtungen (§ 87 Abs. 1 Nr. 6 BetrVG).

Hier stellt sich nun für die beteiligten Betriebsparteien die anspruchsvolle Aufgabe, Regelungen zu schaffen, die im Einklang mit höherrangigem Recht, insbesondere also auch wieder mit den Wertungen des BDSG und den verfassungsrechtlich zu berücksichtigenden Grundsätzen stehen.

In diesem Zusammenhang lässt es das Bundesarbeitsgericht (BAG) allerdings zu, dass eine Betriebsvereinbarung in Einzelpunkten hinter den gesetzlichen Standards zurückbleibt, solange sie sich im Rahmen der Regelungskompetenz der Betriebspartner hält und die Grundsätze über den Persönlichkeitsschutz des Arbeitnehmers im Arbeitsverhältnis insgesamt hinreichend beachtet.[12]

Wenn sich also die Gesamtregelung in der Zusammenschau aller Einzelpunkte als angemessener Ausgleich zwischen den berechtigten Interessen des Arbeitgebers und den schutzwürdigen Interessen der

Betroffenen darstellt, ist die Vereinbarung wirksam, da (grund)rechtskonform.

Soweit es LossPrevention und seine Data-Mining-Fähigkeiten betrifft, ist allerdings insbesondere bei seiner Markteinführung vereinzelt schon grundsätzlich bestritten worden, dass eine derartige Software überhaupt Gegenstand einer betrieblichen Vereinbarung sein kann:

Die Software ermögliche Methoden der Rasterfahndung, die im Arbeitsleben nichts zu suchen hätten. Die eigentliche Zentralfunktion von LossPrevention, die Leistungs- und Verhaltenskontrolle der Beschäftigten, disqualifiziere das Programm für den betrieblichen Einsatz. Außerdem sei eine lückenlose Überwachung von Beschäftigten stets eine Verletzung des Persönlichkeitsrechts eines Arbeitnehmers. Basierend hierauf ist seinerzeit in der Konsequenz die Forderung erhoben worden, Belegschaftsvertretungen müssten sich einer Einführung von LossPrevention vollständig widersetzen.[13] Kein Raum also für Betriebs- bzw. Dienstvereinbarungen?

Ganz so dramatisch ist es dann wohl doch nicht: Dass die Betriebspartner Regelungen über technische Einrichtungen treffen dürfen (gar müssen), die zur Verhaltens- oder Leistungskontrolle bestimmt sind, ergibt sich bereits unmittelbar aus dem Mitbestimmungstatbestand des § 87 Abs. 1 Nr. 6 BetrVG.

Der Hinweis auf die Rechtswidrigkeit lückenloser Überwachung dagegen ist sicherlich grundsätzlich zutreffend. Allerdings setzt hier ja gerade die inhaltliche Arbeit der Interessenvertretung an: Nämlich durch geeignete Regelungen sicherzustellen, dass z. B. bestimmte Aufzeichnungen nicht stattfinden oder zeitlich limitiert sind, arbeitsrechtliche Sanktionen ausgeschlossen sind oder etwa Leistungskontrollen gänzlich zu unterbleiben haben.

Und soweit es das Argument der unzulässigen Rasterfahndung betrifft, kommt selbst das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) in einem Gutachten zum Einsatz von LossPrevention zu folgender relativierender Einschätzung:

„Eine Vorfeldermittlung aus Gesamtkassendatenbeständen ist nicht generell und von vornherein datenschutzrechtswidrig. Da sie eine hohe Eingriffsintensität auch für Dritte mit sich bringt, müssen konkrete Regelungen vorliegen, die den Schutz des Persönlichkeitsrechts der Betroffenen sicherstellen. Datenschutzgerecht ist demnach eine Betriebsvereinbarung, die den Einsatz von LossPrevention zum Schutz von Interessen der verantwortlichen Stelle nur zulässt, soweit sie entgegenstehende schutzwürdige Interessen der Betroffenen überwiegen. Dabei müssen insbesondere Maßnahmen festgelegt werden, die sicherstellen, dass die schutzwürdigen Interessen der Betroffenen nicht generell hinter den Interessen der verantwortlichen Stelle zurückbleiben."[14]

„Die Regelung der Einführung von DLP-Maßnahmen durch Betriebs-/Dienstvereinbarung ist nicht nur zulässig, sondern faktisch der einzig praktikable Weg."

Die Betriebsvereinbarung muss zur Schaffung der bereits erwähnten angemessenen Gesamtregelung sicherstellen, dass eine Erfassung, Verarbeitung und sonstige Verwendung von personenbezogenen oder personenbeziehbaren Daten nur zu konkret festgelegten und bereits bei Erhebung feststehenden Verwendungszwecken erfolgt (Grundsatz der sogenannten Zweckbindung).

Ihr Inhalt muss des Weiteren den in § 9 BDSG sowie der Anlage zu § 9 BDSG genannten konkreten Anforderungen an die technischen und organisatorischen Maßnahmen genügen. Hier sind insbesondere Regelungen zu den Modalitäten der Datenübermittlungen, zu den konkreten Schutzmaßnahmen und zur Zugriffsberechtigung wichtig.

Und sie muss schließlich auch hinreichende Regelungen über die Sicherstellung der gesetzlichen Rechte der von der Datenverarbeitung Betroffenen (im Wesentlichen geregelt in den §§ 33–35 BDSG) enthalten. Hierzu zählen insbesondere verständliche Informationen über die wesentlichen Funktionen der Software, Zweck und Umfang der Datenverarbeitung sowie die konkreten Folgen der Datennutzung.

Fazit

Festzuhalten bleibt, dass die Regelung der Einführung von DLP-Maßnahmen wie der hier vorgestellten durch Betriebs-/Dienstvereinbarung nicht nur zulässig, sondern faktisch der einzig praktikable Weg ist. Da mit einer entsprechenden Vereinbarung jedoch erst eine Rechtsgrundlage für die mit ihnen verbundene Beeinträchtigung von Arbeitnehmerinteressen geschaffen wird, ist es allerdings auch um so wichtiger, dass sich Interessenvertretungen die notwendigen datenschutzrechtlichen Grundkenntnisse verschaffen, um die schützenswerten Belange der Kollegen angemessen sachkundig vertreten zu können.

Autor

Jan A. Strunk ist Rechtsanwalt, Fachanwalt für Informationstechnologierecht sowie für Arbeitsrecht, Seminarreferent & Fachautor und Partner bei Strunk, Dirks + Partner – Kanzlei für Wirtschaft & Arbeit, Informationstechnologie und Medien in Kiel; fon 0431 53013203, strunk@sdplegal.de, www.sdplegal.de

Fußnoten

1 Beispiele bei Joe Meier, Informationsschutz durch Data Loss Prevention, in diesem Heft
2 Für einen weiterführenden Einblick in einschlägige Produkte sei beispielhaft auf folgende Internetseiten verwiesen: www.epicor.com/germany/Solutions/Pages/LossPrevention.aspx, www.aspectlp.com
3 Nähere Infos dazu auf der Anbieterseite: http://ch.fujitsu.com/de/retail/loss_prevention.html
4 http://ch.fujitsu.com/de/retail/loss_prevention.html
5 Siehe hierzu auch Hirsch, Verbrecherjagd mit Data-Mining, in: CuA 3/2010, 27 ff.
6 Vgl. hierzu etwa Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 127 mit weiteren Nachweisen
7 Däubler, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Auflage, 2010, § 32 Rn. 13; Gola/Schomerus BDSG, § 32 Rn. 11
8 Däubler, NZA 2001, 874
9 Gola/Schomerus, aaO., § 32 Rn. 24
10 Wedde, in: Däubler/Klebe/Wedde/Weichert, aaO., § 32 Rn. 127; Gola/Schomerus, aaO., § 32 Rn. 26
11 Weichert, in: Däubler/Klebe/Wedde/Weichert, aaO., § 4 Rn. 2; Gola/Schomerus, aaO., § 4 Rn. 10
12 BAG, Beschluss vom 27.5.1986, Az.: 1 ABR 48/84
13 Grundlegend: Wilke, Rasterfahndung an der Supermarktkasse, in: Computer Fachwissen (jetzt: CuA) 9/2002, 4 ff.
14 ULD Schleswig-Holstein, Gutachterliche Stellungnahme zur datenschutzrechtlichen Zulässigkeit des Einsatzes von Fujitsu LossPrevention Management System, 2002, www.datenschutzzentrum.de/wirtschaft/lossprev.htm