Böker, Karl-Hermann

Research Report

Beschäftigtenausweise und Kontrolle von Beschäftigten

Study der Hans-Böckler-Stiftung, No. 355

Provided in Cooperation with:
The Hans Böckler Foundation

Suggested Citation: Böker, Karl-Hermann (2017) : Beschäftigtenausweise und Kontrolle von Beschäftigten, Study der Hans-Böckler-Stiftung, No. 355, ISBN 978-3-86593-264-8, Hans-Böckler-Stiftung, Düsseldorf

This Version is available at:
https://hdl.handle.net/10419/149862

Hans Böckler Stiftung
Mitbestimmung · Forschung · Stipendien

STUDY

Nr. 355 · Februar 2017

BESCHÄFTIGTENAUSWEISE UND KONTROLLEN VON BESCHÄFTIGTEN

Praxiswissen Betriebsvereinbarungen

Karl-Hermann Böker

MF MITBESTIMMUNGS-FÖRDERUNG

BETRIEBS-VEREINBARUNGEN

Dieser Band erscheint als 355. Band der Reihe Study der Hans-Böckler-Stiftung. Die Reihe Study führt mit fortlaufender Zählung die Buchreihe „edition Hans-Böckler-Stiftung“ in elektronischer Form weiter.

Hans Böckler Stiftung
Mitbestimmung · Forschung · Stipendien

STUDY

Nr. 355 · Februar 2017

BESCHÄFTIGTENAUSWEISE UND KONTROLLEN VON BESCHÄFTIGTEN

Praxiswissen Betriebsvereinbarungen

Karl-Hermann Böker

MF MITBESTIMMUNGS-FÖRDERUNG

BETRIEBS-VEREINBARUNGEN

Der Autor

Karl-Hermann Böker, Autor und Berater für Arbeitnehmervertretungen zu den Themen Informations- und Kommunikationstechnologie (IKT), Arbeitszeit und Zeitwirtschaft

Hans-Böckler-Str. 39, 40476 Düsseldorf
Online-Publikation,
Download unter www.boeckler.de/betriebsvereinbarungen

ISBN: 978-3-86593-264-8

Herausgeberin und Redaktion: Dr. Manuela Maschke, Hans-Böckler-Stiftung
Satz: DOPPELPUNKT, Stuttgart

INHALT

ABKÜRZUNGSVERZEICHNIS

BetrVG	Betriebsverfassungsgesetz
BDSG	Bundesdatenschutzgesetz
BMWi	Bundesministerium der Wirtschaft
DV	Datenverarbeitung
HPR	Hauptpersonalrat
HR	Human Ressource (Personalabteilung)
ID	Identifikationsnummer
IT	Informationstechnik
LuftSiG	Luftsicherheitsgesetz
MFP	Multi-Funktions-Printer
MVG	Mitarbeitervertretungsgesetz
MVO	Mitarbeitervertretungsordnung
NDSG	Niedersächsisches Datenschutzgesetz
PersVG	Personalvertretungsgesetz
PKI	Public Key Infrastructure
PIN	Persönliche Identifikationsnummer
RFID	Radio-Frequency Identification
SigG	Signaturgesetz
SigV	Signaturverordnung
UMTS	Universal Mobile Telecommunications System (Mobilfunkstandard)
VO (EG)	Verordnung des Europäischen Parlaments und des Rates
VO (EU)	Verordnung der Europäischen Kommission

INDEX ICONS

→I Die Kennung am Ende des Zitats bezeichnet die Quelle und den Standort der Vereinbarung im Archiv. Sofern blau unterlegt, gelangen Sie direkt zur Vereinbarung in der Online-Datenbank.

ZUSAMMENFASSUNG

Mitarbeiterinnen und Mitarbeiter erhalten Beschäftigtenausweise, mit denen sie sich eindeutig identifizieren: beim Betreten des Betriebsgeländes, gegenüber dem Sicherheitspersonal auf dem Gelände und an Geräten zur Erfassung von Arbeitszeit bzw. Anwesenheit. Speziell für diese Ausweise wurde in den vergangenen Jahren neue Technik entwickelt: Ein Ausweis genügt, um sich bei Zutrittskontrollen, an diversen technischen Geräten und an betrieblichen Fahrzeugen zu identifizieren, um Arbeits- und Pausenzeiten zu erfassen und um in Kantinen und an Automaten zu bezahlen.

Sicherheit gegen alle denkbaren Arten von Bedrohung erlangt sowohl in privaten Unternehmen als auch in öffentlichen Einrichtungen und Verwaltungen wachsende Bedeutung. Die Anlässe sind vielfältig – seien es Terrorangriffe, Brandanschläge und andere Gefahren von außen. Neben dem Materiellen sind auch das unternehmensinterne Wissen und Knowhow sowie insbesondere die IT-Infrastruktur immer wieder Angriffen ausgesetzt. Dem begegnen die Hersteller von Sicherheitstechnik und -software mit neuester Technik, mit neuesten Verfahren und Methoden.

Die vorliegende Auswertung von 46 Betriebs- und Dienstvereinbarungen stellt die Regelungen zu Beschäftigtenausweisen in den Fokus. Sie ergänzt die bisher erschienenen Auswertungen zu Sicherheitstechniken wie Videoüberwachung und Zeiterfassungssystemen, die oft gemeinsam in einer Vereinbarung geregelt werden.

In den vorliegenden Vereinbarungen regeln die betrieblichen Sozialpartner sowohl Grundsätze und Einzelverfahren bei der Anwendung der Ausweise als auch die Nutzung der Beschäftigtendaten. Sie versuchen einen ausgewogenen Ausgleich zu finden, der verschiedene Aspekte berücksichtigt: Sicherheit, Komfort für Beschäftigte und den Schutz der Persönlichkeitsrechte. Offenbar müssen die Beschäftigten in Unternehmen mit hohen (externen) Sicherheitsanforderungen größere Einschränkungen ihrer Persönlichkeitsrechte akzeptieren, denn die Kontrollerlaubnisse dieser Unternehmen sind meist nur minimal eingeschränkt. Aus öffentlichen Verwaltungen liegen mehr Vereinbarungen vor, in denen der Datenschutz und die Verhinderung von Leistungs- und Verhaltenskontrolle überwiegen.

VORWORT

Sicherheitssysteme in Unternehmen und Verwaltungen dienen einerseits dem Schutz des Eigentums vor Diebstahl und Zerstörung; Sicherheitseinrichtungen und -kontrollen verhindern oder reduzieren auch Gefahren für Leib und Leben. Auf der anderen Seite werden nicht selten Persönlichkeitsrechte von Beschäftigten berührt, wenn es um Sicherheit und Kontrolle geht. Moderne Systeme sammeln jede Menge Daten, protokollieren Diverses, erlauben Bewegungsprofile bis hin zu verdeckten Auswertungen und Kontrollen.

Welche Sicherheitsvorkehrungen sind angemessen, wenn es um Schutz und Sicherheit geht? Bei welchen Maßnahmen wird eher mit Kanonen auf Spatzen geschossen? Überzogene Maßnahmen, die z. B. Beschäftigte einem Generalverdacht aussetzen, sollten verhindert, Arbeits- und Alltagserleichterungen unterstützt werden.

Für die Analyse wurden 46 betriebliche Vereinbarungen der Jahre 2007 bis 2016 ausgewertet. Es wird gezeigt, welche Regelungstrends zur Gestaltung bestehen und wie die betrieblichen Akteure das Thema aufgreifen. Mit den Analysen verfolgen wir nicht das Ziel, Regelungen zu bewerten, die Hintergründe und Strukturen in den Betrieben und Verwaltungen sind uns nicht bekannt. Ziel ist es, betriebliche Regelungspraxis abzubilden, Trends aufzuzeigen, Hinweise und Anregungen für die Gestaltung eigener Vereinbarungen zu geben.

Weitere Hinweise finden Sie im Internet unter
www.boeckler.de/betriebsvereinbarungen

Wir wünschen eine anregende Lektüre!

Dr. Manuela Maschke

1 RAHMENBEDINGUNGEN

Sicherheit gegen alle denkbaren Arten von Bedrohung scheint in deutschen Wirtschaftsunternehmen, öffentlichen Einrichtungen und Verwaltungen steigende Priorität zu erlangen. Bedrohungen werden auf mehreren Ebenen identifiziert: seien es Terrorangriffe, Brandanschläge und andere Gefahren von außen oder Angriffe „von innen", aus den Reihen der Beschäftigten. Je unpersönlicher die Organisationen werden, desto größer wird die Angst vor dem Einzelnen. Neben dem Materiellen sind auch das unternehmensinterne Wissen und Know-how sowie insbesondere die IT-Infrastruktur immer wieder Angriffen ausgesetzt.

Dem begegnen Hersteller von Sicherheitstechnik und -software mit neuesten Sicherheitstechniken, -verfahren und -methoden. Mit dem Blick auf die Bedrohungslage wird die IT-Technik „hochgerüstet", sei es bei Gebäude- und Zutrittskontrollen, Anwesenheitserfassung, Daten- oder Internetverbindungen. Als ein grundlegendes Element der Sicherheit erhalten die Beschäftigten Ausweise ausgehändigt, mit denen sie sich gegenüber dem Sicherheitspersonal und an elektronischen Erfassungsgeräten eindeutig identifizieren können. Die Ausweise sind zum Zweck der Sichtkontrollen mit identifizierenden Texten oder auch einem Foto bedruckt und enthalten im Inneren zum Zweck der technischen Kontrollen diverse elektronische Funktionen und Daten.

Speziell für die Ausweise wurden in den vergangenen Jahren neue Techniken entwickelt. So ist beispielsweise eine sichere berührungslose Identifizierung der Ausweise möglich, wenn sie auch in größeren Entfernungen an Lesegeräten vorbeigeführt werden. Sie können auf einem Chip unterschiedliche elektronische Komponenten und Techniken für verschiedene Anwendungen enthalten. Dies macht es möglich, dass den Beschäftigten ein einziger Ausweis ausgehändigt wird, mit dem sie sich sowohl bei Zutrittskontrollen als auch an diversen technischen Geräten sowie an betrieblichen Fahrzeugen identifizieren, ihre Arbeits- und Pausenzeiten erfassen und in Kantinen und an Automaten bezahlen. Die erhöhte Sicherheit wird so mit verbessertem Komfort für die Beschäftigten kombiniert.

Letztere erhalten mittels der Ausweise die für ihre betrieblichen Aufgaben notwendigen Zutrittsberechtigungen, den Zugang zu Geräten und die Erlaubnis für Funktionen und Datenzugriffe, die sie für ihre Arbeit benötigen. Zugleich wird alles, was nicht unbedingt benötigt wird, unterbunden. Dies gilt sowohl für die Bewegungsfreiheit innerhalb des Betriebsgeländes als

auch für die Zugänge zur betrieblichen Informationstechnik, zu Geräten, Software, Daten und Internetverbindungen.

Die Unternehmen und Verwaltungen führen diese elektronischen Ausweise überwiegend ein, um die Sicherheit für die Betriebe und ihre Beschäftigten zu erhöhen. In zunehmend mehr Branchen und Arbeitsgebieten fordern zudem externe Zertifizierungsstellen erweiterte Sicherheitskontrollen; fehlende Zertifizierungen können dazu führen, dass den Unternehmen Aufträge nicht erteilt oder entzogen werden. Nicht zu verkennen ist allerdings auch, dass mittels der Ausweise und Kontrollmöglichkeiten dem materiellen und geistigen Diebstahl und Vandalismus durch Beschäftigte vorgebeugt werden soll.

In den vorliegenden Vereinbarungen regeln die betrieblichen Sozialpartner a) teilweise in knapper Form einzelne Anwendungen der Ausweise, b) teilweise Grundsätze zur Anwendung der Ausweise und der Beschäftigtendaten, die dabei erhoben, gespeichert und verwendet werden, c) teilweise aber auch in sehr ausführlicher Form alle Aspekte der unterschiedlichen Anwendungen, Techniken und damit verbundenen Verfahren im Umgang mit den Ausweisen. Sie versuchen dabei in der Regel, einen ausgewogenen Ausgleich zu finden, der die Sicherheitsaspekte, den Komfort für die Beschäftigten und die Persönlichkeitsrechte berücksichtigt. Offenbar müssen die Beschäftigten in Unternehmen mit hohen (externen) Sicherheitsanforderungen größere Einschränkungen ihrer Persönlichkeitsrechte akzeptieren, denn die Kontrollerlaubnisse dieser Unternehmen sind meist nur minimal eingeschränkt. Aus öffentlichen Verwaltungen liegen hingegen mehr Vereinbarungen vor, in denen der Datenschutz und die Verhinderung von Leistungs- und Verhaltenskontrolle überwiegen.

2 REGELUNGSINHALTE

Wer mehr wissen möchte
Auszüge aus Vereinbarungen und Recherchemöglichkeiten zu diesem Thema finden sie hier:
http://www.boeckler.de/cps/rde/xchg/hbs/hs.xsl/4129.htm?bvdoku.theme=175

2.1 Ausweise und Technik

Wer mehr wissen möchte
http://www.boeckler.de/cps/rde/xchg/hbs/hs.xsl/4129.htm?bvdoku.theme=175#bvdoku1

In diesem Kapitel werden in knapper Form die unterschiedlichen Arten und Techniken der Beschäftigtenausweise sowie der Computersysteme zur Erfassung, Verarbeitung und Kontrolle von Beschäftigten und deren Daten vorgestellt. Die eigentliche Bedeutung von Beschäftigtenausweisen liegt in der computergestützten Zutrittskontrolle sowie der Sichtkontrolle, die durch offenes Tragen von Ausweisen mit Foto des Beschäftigten möglich wird.

2.1.1 System-Komponenten

Unter den vorliegenden Vereinbarungen regelt nur eine einzige einen nicht computerlesbaren Ausweis:

> „Der Mitarbeiter/innen-Ausweis ist nicht maschinenlesbar und enthält auch keine Ortungsfunktion."
> →| Gesundheit und Soziales, 090600/211/2012

Die Vereinbarung enthält keine Informationen darüber, von wem und wie die Ausweise hergestellt werden; individualisiert werden sie durch Namen und Foto der Beschäftigten.

Bei computerlesbaren Ausweisen, die Regelungsgegenstand der weiteren vorliegenden Vereinbarungen sind, ist der Ausweis lediglich eine Komponente eines umfangreichen Computersystems (auch wenn dies nicht in jeder Vereinbarung deutlich wird). Die Ausweise müssen mittels Computersoftware und -hardware individualisiert werden. Dies geschieht durch Speicherung von eindeutigen Daten in dem Ausweis. Zusätzlich können in dem Ausweis weitere Daten gespeichert werden, die für verschiedene Funktionen verwendbar sind (siehe im Folgenden). Zur Identifizierung der Ausweis-Eigentümer werden Lesegeräte („Terminals“) eingesetzt, die in der Lage sind, die Daten der Ausweise zu erkennen und zu interpretieren. Von den Terminals werden die Daten an spezielle Computersoftware übertragen, die für die Speicherung und weitere Verarbeitung der Daten zuständig sind. Durch Zugriff auf diese Software ist es möglich, die Daten auszuwerten. Da in der Regel nicht jede Person dazu berechtigt sein soll, verfügt die Software über eine Verwaltung von Zugriffsberechtigungen. Über Verbindungen zu anderen Computer- und -Softwaresystemen ist es grundsätzlich möglich, die Daten zu übertragen und beliebig weiterzuverarbeiten. Insgesamt stellt somit der Beschäftigtenausweis nur das Medium dar, mit dem individuelle Daten von Beschäftigten in ein Computersystem eingelesen werden. Beschäftigtenausweise sind zumeist Plastikkarten in der Größe einer Kreditkarte oder als sogenannte Transponder als Schlüssel oder Schlüsselanhänger gestaltet.

2.1.2 Transponder

Ein Transponder ist ein Funk-Kommunikationsgerät, das eingehende Radarsignale aufnimmt und automatisch beantwortet bzw. weiterleitet. Der Begriff Transponder setzt sich aus „Transmitter“ und „Responder“ zusammen. Transponder werden unter anderem als Schlüsselersatz in computergestützten Schließ- und Zutrittskontrollsystemen verwendet, die die mechanischen Schließzylinder ersetzen. Dabei sendet ein Abfragegerät (Türschloss, Terminal etc.) ein Datensignal, das der Transponder mit dem Senden der in ihm gespeicherten Identifizierungsnummer erwidert:

> „Auf dem Transponder ist nur die Identifizierungs-Nummer gespeichert.“
> ➔ Öffentliche Verwaltung, 090600/120/2008

Derartige Systeme können beliebig viele Schlösser und Benutzer verwalten und auch spezielle Steuerungs- und Überwachungsfunktionen enthalten, z. B. zeitabhängige Zutrittssteuerung und Protokollierung.

Sollte ein Transponderschlüssel verloren gehen, so wird dieser einfach gesperrt. Es ist daher, im Gegensatz zu mechanischen Schließanlagen, nicht notwendig alle Schlösser auszutauschen, um einem Missbrauch des verlorenen Schlüssels vorzubeugen[1]. Transponder können außerdem zu anderen Zwecken eingesetzt werden (vgl. Kapitel 2.6).

2.1.3 Ausweiskarte

Beschäftigtenausweise in Kartenform sind entweder mit einem Magnetstreifen oder einem Chip (oder mit beidem) ausgestattet, um computerlesbare Daten zu speichern. Ein Chip kann in mehrere Segmente unterteilt sein, um unterschiedliche Funktionen bedienen zu können:

> „Die einzelnen Anwendungen sind in der Steuerung voneinander unabhängig und auf dem Ausweis in separaten Segmenten codiert. Die Ausweisnummer ist für alle Anwendungen gleich."
>
> →| Maschinenbau, 090501/210/2013

Ausweiskarten können für das berührungslose Authentifizieren – ebenso wie die Transponder – Signale an einen Sender (Terminal) übermitteln. Einige Karten besitzen einen Magnetstreifen, über den beim Durchziehen der Karte Daten an das Terminal übermittelt werden; oder sie enthalten einen Chip, der Daten speichert und durch Einstecken der Karte in das Terminal übermittelt. Zudem ist es möglich, Daten vom Terminal auf den Chip zu übertragen und dort zu speichern. Die modernste Form der Ausweiskarten enthält mehrere Chips für die unterschiedlichen Anwendungen: Neben der Zutrittskontrolle können z. B. auch Zeiterfassung und Bezahlung damit erfolgen oder die Karte zur digitalen Signatur eingesetzt werden. Insbesondere öffentliche Verwaltungen und Bildungseinrichtungen verwenden die Karten zur Authentifizierung im Zusammenhang mit der digitalen Signatur:

1 Informationen erstellt auf der Grundlage von Einträgen in der deutschen Wikipedia-Enzyklopädie, https://de.wikipedia.org/wiki/Transponder, Abruf am 16.01.2017

> „Der Mitarbeiterausweis ist eine multifunktionale Chipkarte (Smartcard), der grundsätzlich als Sichtausweis fungiert."
> ➔I Branchenübergreifend, 090600/127/2009

Zu den weiteren Funktionen siehe Kapitel 2.6.

In einigen Vereinbarungen wird die Technik der Karten genau benannt. Es handelt sich dann beispielsweise um MIFARE DESFire-Karten (→ Glossar), Karten mit RFID-Chip (→ Glossar) oder mit intelligentem Speicherchip vom Typ LEGIC advant (→ Glossar):

> „Die [Karte/Stadt] ist eine RFID-Chipkarte mit einem intelligenten Speicherchip (Typ LEGIC advant) im Kartenkörper. Sie ist eine sog. kontaktlose Chipkarte, bei der der Chip von außen nicht sichtbar in den Kartenkörper eingefügt ist und bei Bezahl- und/oder Anmeldevorgängen über eine ebenfalls in den Kartenkörper integrierte Antenne mit einem Kartenleser des jeweiligen Zielsystems in Verbindung tritt."
> ➔I Bildungseinrichtung, 090600/162/2013

Seltener, überwiegend für Anwendungen mit höheren Sicherheitsanforderungen kommen biometrische Ausweise zum Einsatz. Biometrische Verfahren verwenden, wie in der folgenden Vereinbarung beschrieben, die Fingerabdrücke der Beschäftigten oder die Augen (Iris, Netzhaut) zur Authentifizierung:

> „Bei dem biometrischen Identifikationssystem der [Firma] wird mit elektronischen Mitteln ein Fingerabdruck aufgenommen und dessen wesentliche Ausprägungen mit abgespeicherten Referenzdaten verglichen. Das System verarbeitet mittels Fingerabdrucksensoren die Fingerabdrücke von Mitarbeitern. Referenzdaten sind insbesondere die sogenannten Minuten, welche die relevanten Punkte des Fingerabdrucks charakterisieren. Diese Merkmale sind besonders die Verzweigungsstellen der Furchen und Stege der Hautoberfläche."
> ➔I Kreditgewerbe, 090600/188/2013

Aufgrund der meist großen Akzeptanzprobleme werden die technischen Details, das Verfahren der Authentifizierung sowie die Sicherungsmerkmale in den Vereinbarungen genau beschrieben.

Ausweiskarten werden regelmäßig auf Vorder- und evtl. auch Rückseite bedruckt, damit sie auch zur Sichtkontrolle geeignet sind und den berechtigten Inhaber authentifizieren. Viele Vereinbarungen beschreiben sehr genau, welche Informationen auf den Ausweiskarten zu sehen sind:

> „Jeder [Firmen]-Mitarbeiter erhält einen Mitarbeiterausweis mit folgenden Angaben:
> Vorderseite:
> – Name (Vor- und Nachname) gem. Global-ID-Datenbank (engl. Schriftweise),
> – Global ID (Personalnummer),
> – Lichtbild in Farbe (abgebildetes Gesicht)
> Rückseite:
> – ID-Kartennummer (Ausweisnummer).“
> →| Maschinenbau, 090501/210/2013

Gelegentlich werden den Vereinbarungen Abbildungen der Ausweise als Anlage hinzugefügt. Auch der Aufdruck der Ausweise ist meist in einer Anlage zur Vereinbarung enthalten; dies ermöglicht ein unkompliziertes Aktualisieren bei Veränderungen, ohne die Vereinbarung kündigen zu müssen (vgl. Kapitel 3.1):

> „Seine Gestaltung und Verwendung sowie technische Details und Verfahren ergeben sich aus den Anlagen.“
> →| Maschinenbau, 090600/189/2013

Zu besonderen Regelungen im Zusammenhang mit den verwendeten Fotos siehe Kapitel 2.3.2.

2.1.4 Systembestandteile

Die Ausweiskarten oder Transponder sind nur der für alle Beschäftigte sichtbare Teil eines umfassenden Computersystems. Zu deren Funktionieren benötigt das Unternehmen bzw. die Verwaltung ein technisches System, das aus mehreren Bestandteilen besteht:

„Hardware-Ausstattung für die Anwendung:
Kartenlesegeräte, elektromagnetische Türöffner, Steuereinheiten, Anwendungssoftware, Server."
→| Bildungseinrichtung, 090600/119/2008

Größere Unternehmen und Verwaltungen verfügen über ein Kartenmanagementsystem als zentrale Bedien- und Steuerungssoftware. Auch dies kann in den Vereinbarungen im Detail beschrieben und festgelegt werden:

„Das zugrunde liegende Kartenmanagementsystem dient der Erstellung und Verwaltung der multifunktionalen Mitarbeiterausweise. Jeder Ausweis ist mit einer eindeutigen Kartennummer versehen. Das Kartenmanagementsystem verfügt über eine eigene Personalstammdatenbank und stellt den eindeutigen Bezug zwischen Kartennummer und den Personendaten des Ausweisinhabers her. Es besteht aus folgenden Komponenten:
– Serverumgebung
– Ausweisdrucker (mit Kartenkodierung)
– Schreiblesegeräte
– Bedienstationen (Endgeräte mit Zugang zum Kartenmanagementsystem)."
→| Branchenübergreifend, 090600/127/2009

Die Komponenten sowie alle wesentlichen spezifischen Parameterwerte werden in einigen Vereinbarungen vollständig aufgelistet. Damit ist das zu regelnde System in seiner Gesamtheit dokumentiert und darf nicht ohne Mitbestimmungsverfahren verändert bzw. erweitert werden. Meist finden sich derartige Dokumentationen in einer Anlage zur Betriebs- bzw. Dienstvereinbarung:

„Die Hard- und Softwareausstattung ergibt sich aus der Beschreibung in der Anlage […] zu dieser Betriebsvereinbarung."
→| Datenverarbeitung u. Softwareentwicklung, 090600/210/2013

„Die Systemeinstellungen sind vollständig in der Anlage […] dokumentiert."
→| Öffentliche Verwaltung, 090600/120/2008

Zum Computersystem gehören meist auch Schnittstellen, über die Stammdaten der Beschäftigten in das System übertragen werden. Auch dies ist möglichst genau – beispielsweise in einer Anlage zur Vereinbarung – zu dokumentieren, um den Datenfluss kontrollierbar zu halten:

> „Die für die elektronische Anwesenheitserfassung erforderlichen Stammdaten (Anlage […]) sind aus [der Firma] zur Verfügung zu stellen (zertifizierte Schnittstelle)."
> ➔I Kohlebergbau, 090600/176/2013

Über Schnittstellen können die erhobenen Daten ebenso exportiert werden. Regelmäßig ist dies jedoch durch die Vereinbarung strikt ausgeschlossen, um Datenmissbrauch zu verhindern (vgl. Kapitel 2.7.2). Die Sicherheit gegen Missbrauch und Manipulation steht im Fokus vieler Vereinbarungen. Die Systemkomponenten sollen dementsprechend sehr gut gesichert ausgestaltet werden:

> „Die Elemente des Systems werden entsprechend den zur Verarbeitung gelangenden besonders schutzwürdigen personenbezogenen Daten der Beschäftigten in nach dem jeweiligen Stand der Technik vor unbefugten Zugriffen strikt gesicherten DV-Netzen und -Umgebungen betrieben."
> ➔I Bildungseinrichtung, 090600/162/2013

Zur weiteren Sicherung der Systeme gegen missbräuchliche Nutzung werden zusätzlich kryptografische Verfahren eingesetzt (vgl. Kapitel 2.1.5) und strenge Zugriffsbeschränkungen vorgesehen (vgl. Kapitel 2.5.1).

Den betrieblichen Verhandlungspartnern ist es regelmäßig auch wichtig, die Standorte und die technischen Ausprägungen von Lese- und Erfassungsgeräten (Terminals) festzulegen. Veränderungen sind nur mit Zustimmung der Arbeitnehmervertretung zulässig:

> „Eine aktuelle Übersicht der Standorte der Lesegeräte und die Stellen, an denen die Daten angezeigt werden, werden durch die Personalabteilung im Intranet zur Verfügung gestellt und sind als Anlage 1 Bestandteil dieser Betriebsvereinbarung."
> ➔I Kohlebergbau, 090600/176/2013

Zutrittskontrollsysteme werden teilweise mit Videoüberwachungssystemen kombiniert. Dies kann auch zur Erkennung von Kfz-Kennzeichen bei Ein- und Ausfahrten von Parkplätzen oder Betriebsgeländen genutzt werden (vgl. Böker 2009).

2.1.5 Daten

Grundsätzlich lassen sich drei Datenarten unterscheiden: Systemdaten, Berechtigungsdaten und Ereignisdaten. Sie können auf den Ausweisen oder in den Systemen gespeichert und verarbeitet werden. Die folgende Vereinbarung schlüsselt diese Daten auf und erläutert sie:

> „Es wird grundsätzlich zwischen 3 Datenarten unterschieden:
> – Systemdaten: Netzwerksoftware, Betriebssystem, Programmdateien und Protokolldateien gemäß der besonderen Zweckbestimmung des [Datenschutzgesetzes].
> – Berechtigungsdaten: Identifikationsnummer der Chipkarte, bestimmungsgemäße Zuordnung der Berechtigung […], Zuordnung der Identifikationsnummer der Chipkarte zum Benutzer, Angaben zum Chipkarteninhaber.
> – Ereignisdaten: personen-, orts- und zeitabhängige Daten der Chipkartenbenutzung, Anzahl der Benutzungsversuche."
> →I Bildungseinrichtung, 090600/119/2008

Um eine größtmögliche Datensicherheit zu erreichen, regeln einige Vereinbarungen weitere Details: beispielsweise den Ort und die Dauer der Speicherung sowie eine Verschlüsselung der Daten auf dem Beschäftigtenausweis, während der Benutzung und in den Computersystemen:

> „Der Speicherort, die Art und Weise der Speicherung und die Dauer der Speicherung der betreffenden Daten sind in den jeweiligen Anlagen festgelegt."
> →I Bildungseinrichtung, 090600/119/2008

> „Aufgrund der Sensibilität der Daten für obige Anwendungen sind der Datenschutz und die Datensicherung die wichtigsten Kriterien beim Betrieb des elektronischen Dienstausweises und der damit verbundenen Funktionen. Daher kommen in der Chipkarte ausschließlich Funksysteme nach dem neusten Stand der Technik sowie ein eigenständiger Kryptoprozessor für hochgradig verschlüsselte Datenübertragungen zum Einsatz."
>
> ➔I Bildungseinrichtung, 050310/69/2010

Zusätzliche Sicherheit bei der Benutzung von Beschäftigtenausweisen bietet eine nur dem Inhaber bekannte persönliche Identifikationsnummer (PIN), die bei besonders zu schützenden Anwendungen einzugeben ist:

> „Für den jeweiligen Anwendungsfall kann die Verwendung einer PIN festgelegt werden."
>
> ➔I Bildungseinrichtung, 090600/119/2008

Einige Vereinbarungen legen zudem genau fest, welche Daten bei der Benutzung des Beschäftigtenausweises gespeichert werden. Damit wollen die betrieblichen Vertragspartner in der Regel erreichen, dass keine zusätzlichen Daten gespeichert werden, die zu einer Leistungs- und Verhaltenskontrolle missbraucht werden könnten (vgl. Kapitel 2.4.4):

> „Die Erhebung und Speicherung folgender Zutrittsdaten im systemeigenen Speicher bzw. Server ist zulässig:
> – Datum
> – Uhrzeit
> – Karten-Ausweis-Nr."
>
> ➔I Nachrichtentechnik/Unterhaltungs-, Automobilelektronik, 090600/174/2013

Insgesamt wird deutlich: Die betrieblichen Vertragspartner zahlreicher vorliegender Vereinbarungen legen großen Wert auf eine detaillierte Dokumentation und Regelung der Komponenten im Zusammenhang mit den Beschäftigtenausweisen. Allerdings ist diesbezüglich eine große Diskrepanz zwischen den Dienstvereinbarungen öffentlicher Stellen wie z. B. Bildungsträgern (Universitäten) und den Betriebsvereinbarungen aus der Privatwirtschaft erkennbar (vgl. Kapitel 4).

2.2 Verfahren zur Handhabung von Beschäftigtenausweisen

Wer mehr wissen möchte
Auszüge aus Vereinbarungen und Recherchemöglichkeiten zu diesem Thema finden sie hier:
http://www.boeckler.de/cps/rde/xchg/hbs/hs.xsl/4129.htm?bvdoku.theme=175#bvdoku1

Dieses Kapitel zeigt, welche Regelungen und Verfahren rund um die Handhabung von Beschäftigtenausweisen vereinbart werden. Die meisten Vereinbarungen regeln detailliert alle Verfahrensschritte: vom Erstellen, der Ausgabe und der Verwaltung der Beschäftigtenausweise über das sichtbare Tragen und die Handhabung der Ausweise und alle denkbaren Störfälle bis hin zur Rückgabe bei Ausscheiden aus dem Unternehmen. Diese Regelungen sind notwendig, damit die Beschäftigten Sicherheit im Umgang mit den Ausweisen erhalten.

2.2.1 Verwaltung

Beschäftigtenausweise, egal in welcher Form, müssen hergestellt, individualisiert, an die Beschäftigten ausgegeben, verwaltet und beim Ausscheiden aus dem Unternehmen wieder zurückgenommen und vernichtet werden. Dies sind sicherheitskritische Vorgänge, die zumeist in den Unternehmen selbst durchgeführt werden. Die dafür zuständigen und verantwortlichen Stellen oder Personen werden in Vereinbarungen genannt. Die meisten Vereinbarungen regeln dies sehr genau, wie die folgenden Textauszüge zeigen. Eine detaillierte Darstellung aller in diesem Zusammenhang notwendigen und zulässigen Aufgaben findet sich in einem Textauszug, der aufgrund der Länge nur in der Online-Datenbank der Hans-Böckler-Stiftung verfügbar ist:

Herstellung

> „Der Werksausweis wird in der Ausweisstelle ausschließlich von [Firmen]-eigenem Personal erstellt mit geeigneter IT-Unterstützung."
> ➔I Maschinenbau, 090600/189/2013

Individualisierung

„Der Mitarbeiterausweis ist Eigentum des Unternehmens und personengebunden."

→I Verlags- und Druckgewerbe, 090501/180/2013

„Die Personalisierung und Ausgabe der Mitarbeiterausweise erfolgt ausschließlich durch einen Systemadministrator. Die Personalisierungsanlage ist vor dem Zugriff unberechtigter Personen durch hinreichende Maßnahmen zu schützen."

→I Bildungseinrichtung, 090600/119/2008

Ausgabe

„Für den Zutritt zu den Geschäftsräumen der [Firma] über das Zutrittskontroll-System und zur Nutzung des Zeiterfassungssystems erhält jeder Mitarbeiter einen Transponder. Die Transponder sind Eigentum des Unternehmens und werden den Mitarbeitern kostenlos für die Dauer ihrer Betriebszugehörigkeit zur Verfügung gestellt."

→I Nachrichtentechnik/Unterhaltungs-, Automobilelektronik, 090501/197/2014

„Jeder Mitarbeiter erhält kostenlos einen Betriebsausweis, der nur persönlich zu benutzen ist und auf dem

- der Name,
- die Personalnummer und
- ein Foto

des Mitarbeiters erkennbar sind."

→I Kohlebergbau, 090600/176/2013

Empfang

„Der Empfang des Dienstausweises wird von den Beschäftigten quittiert. Auf der Quittung befinden sich die Kartennummer, der Name des/der Beschäftigten und das Datum der Ausgabe."

→I Bildungseinrichtung, 050310/69/2010

Verwaltung

„Die Verwaltung der Ausweiskarten und die Pflege der personenbezogenen Daten aller der in dieser Vereinbarung genannten personenbezogenen Daten erfolgt durch die Personalabteilung bzw. IT."

→I Datenverarbeitung u. Softwareentwicklung, 090600/210/2013

„Die technische Verwaltung der […]-Chipkarten erfolgt über ein zentrales Kartenmanagementsystem, welches hinsichtlich der Punkte Datensicherheit und Datenschutz sowohl technisch als auch organisatorisch hinreichend sicher zu gestalten ist."

→| Bildungseinrichtung, 090600/119/2008

Der Zugang und Zugriff zu den Systemen, mit denen diese Aufgaben erledigt werden, ist dem entsprechend geschützt:

Ruhendes Arbeitsverhältnis

„Für Mitarbeiter, die sich in einem ruhenden Arbeitsverhältnis befinden, verwahrt die Abteilung Standortmanagement/Factory Site Management die Ausweise bis zur Rückkehr. Dies gilt z. B. für Mitarbeiter in Elternzeit größer 2 Monate, im Abbau von Langzeitkonten, im Bundesfreiwilligendienst, bei Austritt mit Wiedereinstellungszusage. Mitarbeiter in der Altersteilzeit Freistellungsphase müssen den Werksausweis abgeben."

→| Maschinenbau, 090501/210/2013

Rückgabe/Rücknahme

„Beim Ausscheiden aus dem Betrieb ist der Mitarbeiterausweis der Personalabteilung unaufgefordert am letzten Anwesenheitstag im Betrieb zurückzugeben."

→| Unternehmensbezogene Dienstleistungen, 090600/193/2013

„Mit Rückgabe des elektronischen Schließmediums sind alle personenbezogenen Daten zu löschen."

→| Bildungseinrichtung, 090600/122/2009

2.2.2 Verwendung

Die Handhabung der Beschäftigtenausweise formulieren manche Vereinbarungen im Sinne einer Benutzungsanleitung:

„Bei Betreten oder Verlassen des Standortes und bei der Benutzung von Systemen, welche die Anwendung des Firmenausweises erfordern, identifiziert sich die Mitarbeiterin oder der Mitarbeiter mit dem Firmenausweis."

→| Chemische Industrie, 090600/185/2013

Mehrere Vereinbarungen verweisen hingegen auf spezielle Benutzungsordnungen:

> „Das Verfahren zur Zutrittskontrolle ist in der Verfahrensanweisung ‚Aus- und Rückgabe von Schlüsseln und Zylindern, Ein- und Ausbau von Zylindern' des Unternehmensbereichs Facility Management beschrieben."
> →| Gesundheit und Soziales, 090600/209/2013

Andere Vereinbarungen sind eher rechtlich orientiert und weisen darauf hin, was erlaubt und was verboten ist. So wird in mehreren Vereinbarungen deutlich ausgedrückt, dass die Ausweise nur für den persönlichen Gebrauch bestimmt sind und eine Weitergabe an andere Personen nicht zulässig ist:

> „Der Werksausweis ist sorgfältig aufzubewahren. Er ist Firmeneigentum und darf einem anderen nicht überlassen werden, Missbrauch wird strafrechtlich verfolgt."
> →| Maschinenbau, 090600/189/2013

2.2.3 Benutzungs- und Tragepflicht

In einigen Vereinbarungen wird den Beschäftigten die Pflicht auferlegt, den Ausweis sichtbar zu tragen. Wo dies zwingend vorgeschrieben ist, sind die Beschäftigten angehalten, Personen ohne Ausweis anzusprechen und zur Security zu begleiten. Teilweise resultiert dies aus einer gesetzlichen Forderung, z. B. aus dem Luftsicherheitsgesetz (LuftSiG):

> „§ 10 Zugangsberechtigung
> Die Luftsicherheitsbehörde entscheidet, welchen Personen bei Vorliegen der Voraussetzungen die Berechtigung zum Zugang zu nicht allgemein zugänglichen Bereichen erteilt werden darf oder bei Wegfall der Voraussetzungen zu entziehen ist. Nach Abschluss der Zuverlässigkeitsüberprüfung nach § 7 Abs. 1 kann dem Betroffenen zum Nachweis der Zugangsberechtigung ein Ausweis durch den Unternehmer nach § 8 Abs. 1 oder § 9 Abs. 1 ausgestellt werden. Der Ausweisinhaber ist verpflichtet, den Ausweis in den nicht allgemein

zugänglichen Bereichen offen sichtbar zu tragen und ihn nach Ablauf der Gültigkeitsdauer oder auf Verlangen zurückzugeben. Der Ausweisinhaber darf den Ausweis keinem Dritten überlassen. Sein Verlust ist der Ausgabestelle unverzüglich anzuzeigen. Der Zugang zu den nicht allgemein zugänglichen Bereichen ohne Berechtigung ist verboten."

Nicht immer ist den Vereinbarungen deutlich zu entnehmen, welchen Zweck oder Hintergrund die Regelungen haben. Auch im Ernährungsgewerbe können z. B. gesetzliche Hygieneanforderungen bestehen; doch weist die folgende Vereinbarung nicht darauf hin:

„Während des Aufenthalts in Firmengebäuden ist der Hausausweis jederzeit sichtbar an der Kleidung zu tragen."
→| Ernährungsgewerbe, 090600/148/2007

Feststellbar ist jedoch allgemein, dass die betrieblichen Regelungen bei höheren Sicherheitsanforderungen genauer ausgeführt sind:

„Das sichtbare Tragen des Ausweises beginnt mit dem Betreten des Gebäudes. Unter sichtbarem Tragen wird verstanden, dass eindeutig zu erkennen ist, ob es sich (erkenntlich durch Lichtbild) um einen […]-Mitarbeiter oder um eine sog. externe Person (ohne Lichtbild) handelt. [Die Firma] stellt hierzu geeignete Hilfsmittel zur Verfügung."
→| Datenverarbeitung u. Softwareentwicklung, 090600/210/2013

Ausnahmen von der Tragepflicht werden lediglich aus Gründen der Arbeitssicherheit für einzelne Betriebsteile oder Arbeitsplätze formuliert:

„Nur während der Tätigkeit an laufenden (z. B. Fräs-, Dreh-) und sonstigen offenen Maschinen ist auf Anweisung in Abstimmung mit dem zuständigen Vorgesetzten auf offenes Tragen des Werksausweises zu verzichten."
→| Maschinenbau, 090600/189/2013

Auch hier werden die Konsequenzen von Missachtung dieser Bestimmungen genannt:

> „Ein Missbrauch des Werksausweises kann arbeitsrechtliche Konsequenzen zur Folge haben."
> ➔I Nachrichtentechnik/Unterhaltungs-, Automobilelektronik, 090600/174/2013

2.2.4 Störfälle

Die meisten Vereinbarungen befassen sich ebenfalls ausführlich mit Störfällen. Diese sind: Vergessen, Verlust, Bruch oder Beschädigung des Ausweises bzw. technische Störungen der Systeme.

Technische Defekte

Im einfachsten Fall regeln die Vereinbarungen den unkomplizierten und kostenfreien Austausch beschädigter Beschäftigtenausweise:

> „Defekte oder beschädigte Karten werden auf Kosten der [Firma] ausgetauscht."
> ➔I Datenverarbeitung u. Softwareentwicklung, 090600/210/2013

Einige Vereinbarungen unterscheiden jedoch, ob der Schaden durch Fahrlässigkeit oder durch grob fahrlässiges bzw. vorsätzliches Handeln entstanden ist (siehe im Folgenden).

Mit weitergehenden Störungen am technischen System sowie an den damit in Verbindung stehenden Abläufen befasst sich die folgende Regelung in einer Dienstvereinbarung:

> „Bei Bruch des Sicherheitssystems der Bedienstetenchipkarte bzw. bei Versagen der Sicherheitsmaßnahmen im Zuge der Verwendung der Bedienstetenchipkarte entstehen der/dem Beschäftigten keinerlei Nachteile. Das bezieht sich auf die Bedienstetenchipkarte selbst, die für den Betrieb dazu notwendigen Verwaltungssoftware und die durch Nutzung der Bedienstetenchipkarte generierten Verwaltungsvorgänge."
> ➔I Bildungseinrichtung, 090600/181/2009

Derart ausführliche Regelungen sind jedoch die Ausnahme und nur in Dienstvereinbarungen öffentlicher Einrichtungen zu finden (vgl. Kapitel 4).

Vergessen

Das Vergessen von Ausweisen ist weitaus häufiger geregelt. Dies bleibt jedoch für die Beschäftigten ausnahmslos ohne Folgen; die Vereinbarungen regeln lediglich auf unterschiedliche Art, wie und von wem Ersatzausweise ausgestellt werden oder auf welche andere Weise die Identifizierung der Beschäftigten gesichert werden muss:

> „Mitarbeiter, die ihren Ausweis zu Arbeitsbeginn nicht dabei haben, haben nur über eine Anmeldung am Empfang Zutritt und erhalten dort einen befristet nutzbaren Tagesausweis."
> ➔I Nachrichtentechnik/Unterhaltungs-, Automobilelektronik, 090600/174/2013

Verlust

Geht ein Ausweis verloren, ist es immer die Pflicht des Beschäftigten, dies unverzüglich anzuzeigen. Die Vereinbarungen nennen meist die dafür zuständige Stelle:

> „Die Mitarbeiterin oder der Mitarbeiter hat den Verlust des Firmenausweises umgehend, d. h. ohne schuldhaftes Zögern, der zuständigen Ausweisstelle zu melden."
> ➔I Chemische Industrie, 090600/185/2013

Den Beschäftigten werden bei erstmaligem Verlust regelmäßig keine Kosten berechnet, sondern erst bei mehrmaligem Verlust innerhalb eines bestimmten Zeitraums. Auch hier wird teilweise auf den Unterschied zwischen fahrlässigem, grob fahrlässigem oder vorsätzlichen Handeln hingewiesen:

> „Die Ausweiskarten werden den Mitarbeitern bei der Erstausgabe kostenlos zur Verfügung gestellt. Bei Vertust oder Beschädigung wird für den Ersatzausweis eine Gebühr von 5,00 EUR erhoben, sofern der Mitarbeiter den Verlust oder die Beschädigung gemäß § 276 BGB zu vertreten hat (Vorsatz und Fahrlässigkeit)."
> ➔I Nachrichtentechnik/Unterhaltungs-, Automobilelektronik, 090600/174/2013

Die Verlust-Kosten seitens der Betroffenen liegen allgemein zurzeit zwischen 5 und 20 Euro.

Zum Schutz der Beschäftigten regelt eine Dienstvereinbarung, dass den Beschäftigten keine Beweispflicht auferlegt wird:

> „Im Zweifelsfall obliegt es der Dienststelle, den Beweis zu führen, ob der/die Beschäftigte vorsätzlich oder grobfahrlässig gehandelt hat."
> →| Bildungseinrichtung, 090600/181/2009

Zur besonderen Problematik bei Verlust von Ausweisen mit Bezahlfunktion siehe Kapitel 2.6.5.

2.3 Rechte der Beschäftigten

Wer mehr wissen möchte

Auszüge aus Vereinbarungen und Recherchemöglichkeiten zu diesem Thema finden sie hier:
http://www.boeckler.de/cps/rde/xchg/hbs/hs.xsl/4129.htm?bvdoku.theme=175#bvdoku1

Dieses Kapitel befasst sich mit weiteren Rechten der Beschäftigten, die über die Verfahrens- und Handhabungsregelungen hinausgehen. Die Regelungen befassen sich insbesondere mit der Transparenz gegenüber den Beschäftigten. Über die Daten, die auf den Beschäftigtenausweisen gespeichert sind, und über die Verfahren der Datenverarbeitung sollen die Beschäftigten umfassend informiert sein. Eine besondere Rolle spielen ihre Fotos, sofern diese Bestandteil der Ausweise sind.

Zudem befasst sich dieses Kapitel mit sehr unterschiedlich geregelten Aspekten von Freiwilligkeit, Einverständnis und Gleichbehandlung der Beschäftigten.

2.3.1 Informationsrechte

In den Vereinbarungen werden mitunter ausführliche Informationen über die Ziele, die Funktionsweise und die Bedienung der Ausweise und der technischen Systeme vermittelt:

> „Die Beschäftigten erhalten bei der Ausgabe ein Infoblatt, das über die Einsatzmöglichkeiten des Dienstausweises informiert und auf diese Dienstvereinbarung sowie auf das Verhalten bei Kartenverlust hinweist."
> ➔ Bildungseinrichtung, 050310/69/2010

Bei Beschäftigtenausweisen mit umfangreichen Nutzungsmöglichkeiten reicht eine schriftliche Information allein meist nicht aus, so dass die Vereinbarungen entsprechende Schulungsmöglichkeiten regeln:

> „Die Beschäftigten, die mit der Bedienstetenchipkarte arbeiten, werden ausreichend unterrichtet. Schulungen zu den Funktionen der Bedienstetenchipkarte werden im Rahmen des Weiterbildungsprogramms der [Firma] angeboten."
> ➔ Bildungseinrichtung, 090600/181/2009

Den Beschäftigten wird das volle Einsichtsrecht in die gespeicherten und verarbeiteten personenbezogenen Daten zugestanden; zudem teilweise, wie in folgender Regelung, die Möglichkeit des Daten-Abrufs:

> „Die Beschäftigten haben Anspruch, die erfassten Daten während der Arbeitszeit am Buchungsterminal auf dem Display abzurufen."
> ➔ Kirchen, 090501/181/2011

Vereinzelt werden die Beschäftigten zusätzlich darüber informiert, dass sie keine Nachteile durch die Anwendung des Systems zu befürchten haben:

> „Mitarbeiterinnen und Mitarbeitern dürfen aufgrund der Anwendung des Systems keine Nachteile entstehen. Im Konfliktfall ist die Mitarbeitervertretung einzubeziehen."
> ➔ Gesundheit und Soziales, 090600/209/2013

Bei der Auswertung der vorliegenden Vereinbarungen fällt auch hierzu auf: Dienstvereinbarungen enthalten regelmäßig wesentlich ausführlichere Regelungen zu den Informationsrechten der Beschäftigten (vgl. Kapitel 4).

2.3.2 Lichtbild

Der Ausweis enthält oft ein Lichtbild (Foto) des Beschäftigten. Da die Verwendung von Fotos aus Gründen des Persönlichkeitsschutzes grundsätzlich untersagt ist, müssen die Vereinbarungen die für diesen Zweck begrenzte Erlaubnis enthalten. Die Vereinbarungen regeln dementsprechend regelmäßig den Zweck und die Verwendung des Fotos:

> „Das Lichtbild dient der schnellen Identifizierung des Mitarbeiters. Die Fotos dienen der Erstellung des Werksausweises. Eine darüber hinaus gehende Verwendung des Fotos bedarf der Zustimmung des Mitarbeiters."
> ➔I Maschinenbau, 090501/210/2013

Eine Verwendung des Lichtbildes zu anderen Zwecken ist somit ausgeschlossen. Teilweise regeln die Vereinbarungen zudem die technischen und organisatorischen Maßnahmen zum Schutz der Lichtbilder vor weiterer Verwendung; aber auch zur Erlaubnis, sie bei Ausstellen eines Ersatzausweises verwenden zu dürfen:

> „Sie werden elektronisch in der [Firma] gespeichert, um ggf. bei Verlust einen neuen Ausweis erstellen zu können, eine weitere Nutzung […] ist ohne eine vorherige ausdrückliche Zustimmung des Mitarbeiters ausgeschlossen. Nach Austritt des Mitarbeiters werden diese Daten gelöscht und die Karte vernichtet."
> ➔I Datenverarbeitung u. Softwareentwicklung, 090600/210/2013

2.3.3 Einverständnis, Freiwilligkeit, Gleichbehandlung

Einzelne Vereinbarungen regeln spezielle Aspekte, die hier nicht unerwähnt bleiben sollen. Denn sie können im Einzelfall unter speziellen Rahmenbedingungen relevant sein.

In einer Vereinbarung wird vor Inbetriebnahme des Systems eine Einverständniserklärung der Beschäftigten verlangt. Dies ist bei einem biometrischen System aufgrund der Verarbeitung sensibler personenbezogener Daten (in diesem Fall der Fingerabdruck) notwendig:

> „Vor der Nutzung von Fingerprint ist vom Mitarbeiter die Einverständniserklärung zur Nutzung von biometrischen Daten gemäß § 4 BDSG […] einzuholen."
> ➔ Kreditgewerbe, 090600/188/2013

Einigen Arbeitnehmervertretungen war es offenbar wichtig, die Freiwilligkeit zu betonen:

> „Die Nutzung der elektronischen Schließanlage erfolgt auf freiwilliger Basis. Es bleibt den Dienstkräften unbenommen, das Dienstgebäude ohne Einsatz des Transponders unter Vorlage des Dienstausweises über den Haupteingang zu betreten."
> ➔ Öffentliche Verwaltung, 090600/120/2008

Die Formulierung deutet jedoch darauf hin, dass es mit Nachteilen für die Beschäftigten verbunden sein wird, wenn sie ihr Recht wahrnehmen. Im Gegensatz dazu steht die folgende Formulierung:

> „Der dienstliche Einsatz der Signaturkarte an IT-gestützten Arbeitsplätzen der [Firma] ist nach Einführung verpflichtend."
> ➔ Öffentliche Verwaltung, 090600/158/2009

Die Verwendung der technischen Systeme und der Beschäftigtenausweise lässt in der Regel keine Freiwilligkeit zu. Ähnliches gilt für die in wenigen Vereinbarungen anzutreffende Regelung zur Gleichbehandlung der Beschäftigten:

> „Alle Mitarbeiterinnen haben gleiche Zugangsrechte."
> ➔ Mess-, Steuer- und Regelungstechnik, 090600/201/2013

Meist wird mit den Beschäftigtenausweisen und den damit verbundenen Zugangssicherungssystemen das gleiche Zugangsrecht für alle Beschäftigten

ausgeschlossen, um höheren Sicherheitsanforderungen zu genügen. Dadurch wird auch eine Form von Gleichbehandlung ausgedrückt:

> „Die [Firma] stellt sicher, dass jeder Mitarbeiter über die Zutrittskarte diejenigen Zutrittsrechte erhält, die er zur Erfüllung seiner Aufgaben benötigt."
>
> →| Datenverarbeitung u. Softwareentwicklung, 090600/210/2013

2.4 Persönlichkeitsrechte

Wer mehr wissen möchte
Auszüge aus Vereinbarungen und Recherchemöglichkeiten zu diesem Thema finden sie hier:
http://www.boeckler.de/cps/rde/xchg/hbs/hs.xsl/4129.htm?bvdoku.theme=175#bvdoku1

Dieses Kapitel behandelt rechtliche Regelungen in den vorliegenden Vereinbarungen, die auf Grundlage von Datenschutz- und Mitbestimmungsgesetzen vereinbart werden. Geregelt werden allgemeine Datenschutzrechte und -pflichten, die teilweise in unterschiedlicher Weise detaillierter ausgeführt werden. In einigen Vereinbarungen werden zudem spezifische Aufgaben des betrieblichen Datenschutzbeauftragten geregelt. Eine besondere Rolle spielen die Aufbewahrungsfristen von personenbezogenen und -beziehbaren Daten.

Zusätzlich zu einem grundsätzlichen Verbot von Leistungs- und Verhaltenskontrolle regeln einige Vereinbarungen die speziellen Zugriffsrechte, teilweise auch unter Einbeziehung von Fernzugriffen zu den technischen Systemen, sowie den Umgang mit der Protokollierung von Zugriffsdaten. Die wesentlichen rechtlichen Grundlagen sind in Kapitel 6.3 nachzulesen.

2.4.1 Datenschutz

Eine Dienstvereinbarung stellt grundlegend fest, dass das Datenschutzrecht bei Einführung und Nutzung von Beschäftigtenausweisen zu beachten ist:

> „Bei Einführung und Betrieb des Dienstausweises und der zusätzlichen Funktionen werden personenbezogene Daten verwendet und es entstehen neue Daten, die zum Betrieb neuer Dienste auch notwendig sind. Die Dienststelle verpflichtet sich, die Bestimmungen zum Datenschutz einzuhalten."
>
> ➔ Bildungseinrichtung, 050310/69/2010

Manche Vereinbarungen weisen lediglich darauf hin, dass das anzuwendende Datenschutzgesetz einzuhalten ist. Im folgenden Beispiel wird auf das Niedersächsische Datenschutzgesetz (NDSG) verwiesen:

> „Die nach §7 Abs. 2 NDSG erforderlichen und angemessenen technischen und organisatorischen Maßnahmen des Datenschutzes werden sichergestellt und in dem Berechtigungs- und Sicherheitskonzept dokumentiert. Bei der Gestaltung des Systems werden die Grundsätze der Datenvermeidung und der Datensparsamkeit beachtet sowie die Rechte der Betroffenen (Auskunft, Berichtigung, Sperrung und Löschung) gewährleistet."
>
> ➔ Öffentliche Verwaltung, 090600/158/2009

Derartige Regelungen sind nicht notwendig, da die Einhaltung der Gesetze ohnehin zwingend vorgeschrieben ist. Sie weisen die Beschäftigten und den Arbeitgeber lediglich darauf hin, dass es in diesem Zusammenhang gesetzliche Bestimmungen gibt.

Teilweise enthalten die Vereinbarungen konkrete Bestimmungen zur Umsetzung dessen, was die Datenschutzgesetze fordern. Im folgenden Beispiel wird auf die Anforderungen gemäß §9 Bundesdatenschutzgesetz (BDSG) zum Punkt „Technische und organisatorische Maßnahmen" verwiesen. Im Vereinbarungstext sind dann zu jeder Anforderung aus der Anlage zu §9 BDSG konkrete Ausführungen vorhanden; diese sind in der Online-Datenbank zu dieser Auswertung nachzulesen:

> „Der Arbeitgeber hat die wirksame Umsetzung der nach §9 und Anlage zu §9 BDSG bzw. dem entsprechenden Landesdatenschutzgesetz erforderlichen technischen und organisatorischen Maßnahmen sicherzustellen."
>
> ➔ Kreditgewerbe, 090600/188/2013

Noch genauer regeln andere Vereinbarungen die Zweckbestimmung im Sinne des Datenschutzrechts, indem sie die bei der Nutzung der Ausweise gelesenen und gespeicherten Daten benennen (vgl. Kapitel 2.1.5):

> „Im [Zutrittskontrollsystem] werden von Mitarbeiterinnen nur die Zutritts-Identifikationsnummer, die Berechtigungsprofile für die Türen und die Uhrzeiten der Zutrittsberechtigungen ausgelesen, datentechnisch erfasst und für den zwischen Dienststelle und [Personalrat] vereinbarten Zeitraum gespeichert."
> →I Gesundheit und Soziales, 090600/90/2007

Die maximale Datenvermeidung wird dadurch erreicht, dass bei der Benutzung der Ausweise und Transponder keine Daten gespeichert werden, sondern lediglich die Zugänge freigegeben werden. Sofern dies vereinbart wurde, sind als Ausnahmen meist die Zutritte zu Sicherheitsbereichen, zum Rechenzentrum oder zu vergleichbaren hochsensiblen Bereichen der Unternehmen und Verwaltungen angeführt:

> „Eine generelle Protokollierung der Öffnungsvorgänge an den Onlinetüren findet nicht statt. Ausnahmen davon, bei denen eine Protokollierung sinnvoll und/oder erforderlich ist (z. B. Rechenzentrumszugang), sind in einem Anhang zum Betriebskonzept abschließend aufgeführt."
> →I Gesundheit und Soziales, 090600/90/2007

Die Regelungen zum Datenschutz fallen insgesamt recht uneinheitlich aus. Während einige Vereinbarungen ins Detail gehen, verweisen andere lediglich auf die geltenden gesetzlichen Bestimmungen und den Bezug zu den jeweiligen betrieblichen Aufgaben.

2.4.2 Datenschutzbeauftragte

Der bzw. die betriebliche Datenschutzbeauftragte wird in einigen Vereinbarungen mit seinen bzw. ihren in diesem Zusammenhang zu erledigenden Aufgaben genannt:

> „Die erfassten Daten werden im Rahmen des Datenschutzrechtes und unter Kontrolle des […]-Datenschutzbeauftragten verarbeitet."
> ➔ Ernährungsgewerbe, 090600/155/2011

Diese sind oft weitgehend identisch mit der Rolle der Betriebs- bzw. Personalräte oder gemeinsam mit diesen auszuführen:

> „Der Betriebsrat hat in Zusammenarbeit mit dem betrieblichen Datenschutzbeauftragten über die Einhaltung der genannten Anforderungen zu wachen, Mängel aufzuzeigen sowie auf deren Beseitigung hinzuwirken."
> ➔ Kreditgewerbe, 090600/188/2013

Mehrere Vereinbarungen verweisen darauf, dass Unterweisungen zum Datenschutz durchgeführt werden müssen. Dafür sind, auch ohne dass dies explizit genannt wird, regelmäßig die Datenschutzbeauftragten zuständig:

> „Der mit der Datenverarbeitung beauftragte Betreiber wird verpflichtet, die mit der Verwaltung des Systems betrauten Mitarbeiter über diese Betriebsvereinbarung schriftlich zu belehren und die Einhaltung der Vereinbarung und des Datenschutzes sicherzustellen."
> ➔ Branchenübergreifend, 090600/127/2009

In einer Dienstvereinbarung zu einer Multifunktionskarte mit Signaturfunktion (vgl. Kapitel 2.6.1) wird eine Vorabkontrolle gemäß Landesdatenschutzgesetz verlangt:

> „Aufgrund der sehr hohen technischen Komplexität des Systems ist der Landesbeauftragte für den Datenschutz […] eingebunden, welchem zur Prüfung aller datenschutzrechtlichen Belange des elektronischen Dienstausweises […] eine Vorabkontrolle vorgelegt wird. Erst nach erfolgreichem Abschluss dieser Prüfung wird das System des elektronischen Dienstausweises in den Regelbetrieb überführt."
> ➔ Bildungseinrichtung, 050310/69/2010

2.4.3 Aufbewahrungsfristen

Mehrere Vereinbarungen widmen sich der Festlegung von Aufbewahrungsfristen der personenbezogenen und -beziehbaren Daten: a) die Stammdaten, die für den Beschäftigtenausweis und die damit verbundenen Funktionen notwendig sind, b) außerdem die bei der Benutzung des Ausweises erhobenen Daten und schließlich c) auch die beim Zugang und der Benutzung der verarbeitenden Software anfallenden Bewegungsdaten. Für jede Datenart nennen die Vereinbarungen unterschiedliche – und keineswegs einheitliche – Fristen. Diese liegen zwischen einigen Sekunden und 30 Jahren.

Die Dauer der Datenspeicherung hängt eng mit der Zweckbestimmung der Systeme zusammen. Grundsätzlich können die bei Zutritt zum Unternehmen erhobenen Daten sofort wieder gelöscht werden, sofern nicht geregelt ist, dass diese Daten ggf. bei besonderen Vorkommnissen näher betrachtet werden dürfen:

> „Die an den [Zugangskontroll]-Terminals anfallenden Daten wie Transponder-ID, Datum und Uhrzeit des Zutritts, Terminal-ID werden gemäß Zweckbestimmung zwischengespeichert (kodiert) und innerhalb einiger Sekunden automatisch wieder gelöscht."
> ➔I Nachrichtentechnik/Unterhaltungs-, Automobilelektronik, 090501/197/2014

Im Zusammenhang mit der Aufklärung von Straftaten oder ähnlichen Vorkommnissen ist regelmäßig eine relativ kurze Aufbewahrungszeit der Daten ausreichend:

> „Daten zur Anwesenheit werden nach 14 Tagen automatisch gelöscht, sofern nicht im Einzelfall eine längere Aufbewahrungszeit erforderlich ist."
> ➔I Kohlebergbau, 090600/176/2013

Bestehen – wie in diesem Beispiel angedeutet – konkrete Anhaltspunkte für eine Straftat, wird meist keine Löschfrist mehr gesetzt, sondern auf eine einvernehmliche Verständigung verwiesen:

> „Ergibt sich bei besonderen Vorkommnissen der Bedarf, das Zugangsprotokoll länger zu sichern, kann dies im Einvernehmen mit Betriebsrat und Unternehmensleitung erfolgen."
> ➔ Grundstücks- und Wohnungswesen, 090600/99/2009

Eine längere Aufbewahrung, beispielsweise bis zu 7 Jahren, wird teilweise mit gesetzlichen oder behördlichen Auflagen begründet und steht im direkten Zusammenhang mit der Anwendung der Beschäftigtenausweise – in diesem Fall für eine Arbeitszeiterfassung:

> „Gemäß § 147 Abs. 1 Nr. 5 AO gehören die betrieblichen Zeiterfassungen zu den Lohnberechnungsunterlagen und sind 6 Jahre aufzubewahren."
> ➔ Nachrichtentechnik/Unterhaltungs-, Automobilelektronik, 090501/197/2014

2.4.4 Leistungs- und Verhaltenskontrollen

Grundsätzlich untersagen die Vereinbarungen eine Kontrolle von Leistung und Verhalten der Beschäftigten. Es ist untersagt, aufgrund der erfassten Daten Bewegungsprofile von Beschäftigten zu erstellen:

> „Eine Leistungs- und Verhaltenskontrolle der Mitarbeiter findet nicht statt. Für die benannten Anwendungen dürfen personenbezogene Daten nur nach gesetzlichen Vorschriften, tarifrechtlichen Vereinbarungen und den Regelungen dieser Dienstvereinbarung erhoben, verarbeitet und genutzt werden. So dürfen z. B. personenbezogene Daten, die für eine Verhaltenskontrolle geeignet sind, nicht dafür verwandt werden, individuelle Eigenschaften mit Anforderungsprofilen zu vergleichen."
> ➔ Bildungseinrichtung, 090600/119/2008

Ausnahmen sind regelmäßig zulässig. So können die Unternehmen bzw. Verwaltungen beispielsweise Auswertungen von Daten vornehmen, die im Sinne der untersagten Kontrollmöglichkeiten unbedeutend, für den Arbeitgeber jedoch relevant erscheinen:

> „Diese Daten dürfen nicht zur Leistungs- und Verhaltenskontrolle herangezogen werden, werden jedoch am nächsten Arbeitstag durch die Verantwortlichen des Magazins kontrolliert, wer in dieser Zeit das Magazin bzw. das Kleinteilelager betreten hat."
>
> → Ernährungsgewerbe, 090600/146/2010

Auswertungen im Einzelfall sind regelmäßig zulässig, wenn dies der Aufklärung von Straftaten oder anderweitigen Verfehlungen einzelner Beschäftigter dient. Die folgende Regelung ist dafür typisch:

> „Lassen einzelne Erkenntnisse dennoch Rückschlüsse auf die individuelle Leistung und/oder das individuelle Verhalten von Konzernarbeitnehmern zu, dürfen diese nicht als Anlass und/oder Grundlage für arbeitsrechtliche Maßnahmen verwendet werden. Dies gilt nicht, wenn und soweit die Erkenntnisse strafrechtlich relevant sind, insbesondere ein hinreichend begründeter Verdacht auf eine strafbare Handlung besteht."
>
> → Branchenübergreifend, 090600/127/2009

Weitere Details zu den Regelungen für einzelfallbezogene Auswertungen sind in Kapitel 2.7.4 ausgeführt.

2.4.5 Berechtigungen/Zugriffsregelungen

Zur technischen Umsetzung der Datenschutzanforderungen sind die Softwaresysteme mit einer Berechtigungsverwaltung ausgestattet. Die Vereinbarungen begrenzen die Zugriffsrechte überwiegend auf wenige Personen oder, wie im folgenden Beispiel, auf Sicherheitspersonal:

> „Die Daten, die das Zutrittskontrollsystem erfasst, können nur über einen speziellen Ausweis von Mitarbeitern der [Firma] (Werkschutz) ausgelesen werden."
>
> → Mess-, Steuer- und Regelungstechnik, 090600/201/2013

In einer Vereinbarung, die sich auf Beschäftigtenausweise mit biometrischen Daten bezieht, ist zusätzlich der Zutritt zu den technischen Systemen eng begrenzt:

> „Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen die biometrischen Daten verarbeitet oder genutzt werden, durch den Arbeitgeber zu verwehren."
> ➔ Kreditgewerbe, 090600/188/2013

Nicht bei jeder Anwendung von Beschäftigtenausweisen sind derart hohe Sicherheitsanforderungen angebracht. Üblich ist daher, dass der Kreis von Zugriffsberechtigten und ihrer jeweiligen Rechte in einer Anlage zur Vereinbarung abschließend benannt ist:

> „Der Kreis der zugriffsberechtigten Personen für die Verwaltungssoftware wird unter Beachtung der Zweckbestimmung festgelegt und in Anlage […] dokumentiert."
> ➔ Bildungseinrichtung, 090600/181/2009

Der Zweck der Zugriffsberechtigungen kann wie in der folgenden Regelung eindeutig beschrieben und beispielsweise auf wenige Funktionen begrenzt werden:

> „Von der [Verwaltung] bestimmte Personen werden auf das System ausschließlich zugreifen, um
> – Identifizierungs-Nummern (Transponder) zu sperren,
> – Identifizierungs-Nummern (Transponder) zu aktivieren."
> ➔ Öffentliche Verwaltung, 090600/120/2008

2.4.6 Fernzugriff

Moderne Softwaresysteme sind heutzutage regelmäßig über das Internet und über spezielle Software zum Fernzugriff („Remote") erreichbar. Vielfach werden neue Versionen („Updates") der Software automatisch über das Internet eingepflegt. Lediglich drei Vereinbarungen befassen sich mit diesem Thema; ein Beispiel ist die folgende Regelung:

> „Zur Ferndiagnose und für die Systemwartung kann eine Verbindung zur Hersteller- bzw. Wartungsfirma aufgebaut werden. Alle Transaktionen und Zugriffe sind in geeigneter Form zu protokollieren."
> ➔ Chemische Industrie, 090600/206/2012

Aus Gründen der Datensicherheit und des Datenschutzes sind Internetverbindungen grundsätzlich als bedenklich einzustufen (vgl. Kapitel 4).

2.5 Zutritts- und Anwesenheitskontrollen

Wer mehr wissen möchte
Auszüge aus Vereinbarungen und Recherchemöglichkeiten zu diesem Thema finden sie hier:
http://www.boeckler.de/cps/rde/xchg/hbs/hs.xsl/4129.htm?bvdoku.theme=175#bvdoku1

Dieses Kapitel befasst sich mit dem wesentlichen Zweck der Einführung und Nutzung von Beschäftigtenausweisen: der Kontrolle von Zutritt und Anwesenheit zum bzw. auf dem Betriebsgelände. Die Vereinbarungen regeln meist sehr ausführlich, zu welchen Zwecken, in welchen Bereichen und auf welche Weise Kontrollen im Unternehmen durchgeführt werden sollen und dürfen. Teilweise werden spezielle Grenzen der Kontrolle vereinbart, wie im letzten Abschnitt dieses Kapitels gezeigt wird.

2.5.1 Kontrollzwecke

Unternehmenssicherung
Mit der Einführung von Beschäftigtenausweisen bezwecken die Unternehmen häufig, die Sicherheit für das Unternehmen und für die Beschäftigten zu verbessern. Sicherheit für das Unternehmen besteht demnach darin, dass die Objekte (Gebäude, sicherheitskritische Informationstechnik, Dokumente etc.) geschützt sind:

> „Mit dieser Vereinbarung wird die Einrichtung und Anwendung eines Zugangskontrollsystems zum Zwecke des Objektschutzes geregelt. Das System soll damit das schutzwürdige Interesse des Werkes unterstützen."
>
> →| Ernährungsgewerbe, 090600/146/2010

Etwas genauer gefasst, soll damit unter anderem ein Schutz gegen unbefugtes Betreten und gegen Diebstahl von Material und Know-how erreicht werden. Die folgende Vereinbarung nennt zudem weitere Ziele:

> „Vorliegende Zutrittsregelung
> – schützt das Eigentum und Know-how der [Firma] vor Diebstahl,
> – schützt die betrieblichen Abläufe vor möglichen Störungen,
> – sichert die Umsetzung des Arbeitsschutzes,
> – sichert die Umsetzung der gesetzlichen Sicherheitsvorschriften zum Schutz vor der Bedrohung des Terrorismus bei dem Versand von Luftfracht."
> ➔ Maschinenbau, 090600/168/2013

Der Schutz gegen terroristische Bedrohungen ist insbesondere bei Unternehmen, die im Bereich der Luftfahrt agieren, ein häufig genannter Zweck (vgl. Kapitel 2.8.2).

Beschäftigtensicherheit

Eine höhere Sicherheit für Beschäftigte soll beispielsweise dadurch erreicht werden, dass der Zutritt Unbefugter verhindert wird:

> „Die Einführung der Schließanlage dient ausschließlich der Verbesserung der Sicherheit der Mitarbeiter und der im Betrieb benutzten Einrichtungen durch Verhinderung des Zutritts durch Unbefugte."
> ➔ Grundstücks- und Wohnungswesen, 090600/99/2009

Dies wird durch Regelungen unterstützt, die von den Beschäftigten verlangen, die (mit Lichtbild versehenen) Ausweise offen sichtbar zu tragen (vgl. Kapitel 2.2.3). Laut folgender Regelung ist die Sichtkontrolle sogar der Hauptzweck:

> „Der einheitliche multifunktionale Mitarbeiterausweis dient primär zur visuellen Identifizierung der Zutrittsberechtigten der Gesellschaften im […] Konzern."
> ➔ Branchenübergreifend, 090600/127/2009

Technische Systeme und Beschäftigtenausweise sind manchmal Bestandteil eines umfassenden einheitlichen Sicherheitskonzepts. Unternehmen und

Konzerne mit mehreren Standorten statten dementsprechend ihre Beschäftigten an allen Standorten mit einheitlichen Ausweisen aus.

Externe Anforderungen

Nicht selten werden Beschäftigtenausweise mit externen Anforderungen begründet, beispielsweise seitens der Gesetzgeber. Grundlage für die Beschäftigtenausweise, die zur digitalen Signatur (vgl. Kapitel 2.6.1) verwendet werden sollen, sind das Signaturgesetz (SigG) und die Signaturverordnung (SigV) der Bundesregierung:

> „Für die Funktion der Digitalen Signatur muss die Bedienstetenchipkarte die technischen Anforderungen des Signaturgesetzes SigG und der Signaturverordnung SigV erfüllen."
> →I Bildungseinrichtung, 090600/181/2009

Für einige Branchen sind Sicherheitsmaßnahmen nachzuweisen, um Zertifizierungen zu erhalten oder aber, um überhaupt Aufträge zu bekommen. So muss sich z. B. das Unternehmen, in dem die folgende Regelung gilt, nach dem Geheimschutzhandbuch des Bundesministeriums für Wirtschaft und Energie (BMWi) richten (vgl. BMWi 2014) und die dort geforderten Zutrittskontrollen einrichten:

> „Kontrollzonen sind Unternehmensbereiche (Räume oder Einrichtungen) zur Bearbeitung von Verschlusssachen. Sie sind von [der Firma] auf Verlangen des Bundesministeriums für Wirtschaft und Technologie einzurichten, um den materiellen Geheimschutz sicherzustellen. Näheres regelt das Geheimschutzhandbuch des BMWi, zu dessen Umsetzung jeweils eine Kontrollzonen-Anweisung eine Zutrittskontrolle mit Ausweisleser zwingend vorschreibt."
> →I Maschinenbau, 090600/189/2013

Die Deutsche Gesetzliche Unfallkasse fordert den Einsatz biometrischer Systeme in PLUS-Zweigstellen (→ Glossar) von Banken und Sparkassen:

> „Der Betrieb der Geschäftsstellen nach den Regelungen der Unfallkassen schreibt den Einsatz biometrischer Systeme in PLUS-Stellen vor."
> →I Kreditgewerbe, 090600/188/2013

Das Bundesamt für Luftsicherheit fordert die Einhaltung des Luftsicherheitsgesetzes. Die in diesem Bereich agierenden Unternehmen müssen als „Bekannte Versender“ zertifiziert sein, um Aufträge zu erhalten:

> „Nach den gesetzlichen Bestimmungen (derzeit Verordnung VO (EG) Nr. 300/2008 vom 11. März 2008 in Verbindung mit der Verordnung VO (EU) 185/2010 vom 4. März 2010) können sich Unternehmen, die Produkte per Luftfracht sowohl in Passagier- als auch in Frachtflugzeugen versenden, in einem vom Luftfahrtbundesamt vorgeschriebenen Verfahren als ‚Bekannter Versender’ zertifizieren lassen.“
>
> ➔ Mess-, Steuer- und Regelungstechnik, 090600/186/2012

2.5.2 Kontrollbereiche

In Abhängigkeit von den Kontrollzwecken und -grundlagen regeln die Vereinbarungen, welche Bereiche der Unternehmen bzw. Verwaltungen und welche Personen und Gegenstände kontrolliert werden. Gegen unberechtigten Zutritt zum Betriebsgelände werden die Zugänge und Zufahrten gesichert:

> „Betriebsgelände und Gebäude der [Firma] sind durch bauliche, technische und organisatorische Maßnahmen vor dem Zutritt unbefugter Personen gesichert. Der Zutritt befugter Personen erfolgt nach klaren Regeln.“
>
> ➔ Maschinenbau, 090600/168/2013

Handelt es sich um spezielle Sicherheitsbereiche, z. B. Labore oder Rechenzentren, sind die Zugänge zu einzelnen Gebäuden, Etagen oder Räumen mit Ausweislesern ausgestattet:

> „Das Raumprofil unterscheidet nach Zutrittsberechtigung zu den folgenden Bereichen:
> – […]-Haus generell
> – Räume der Generaldirektion
> – Besonders geschützte IT-Räume.“
>
> ➔ Ernährungsgewerbe, 090600/148/2007

Je höher die Sicherheitsanforderungen sind, desto mehr Kontrolltechnik wird eingesetzt. Zusätzlich zu einem Ausweisleser kann die Eingabe einer PIN gefordert, eine Videokamera installiert oder ein biometrisches Lesegerät vorhanden sein (Näheres über Vereinbarungen zu Videoüberwachung bei Böker 2009):

> „Der Zugang zu bestimmten Gebäuden oder Gebäudeteilen wird ebenfalls über Kartenlesegeräte geregelt und bei sicherheitsrelevanten Bereichen ggf. mit Fischaugenkameras und Überwachungsmonitoren ausgestattet."
> ➔I Chemische Industrie, 090600/206/2012

Zusätzlich können die Zugänge mit zeitlichen Einschränkungen versehen sein:

> „Mit Hilfe des Transponders wird jeder berechtigten Dienstkraft in der Zeit montags bis freitags zwischen 5:30 und 20:30 Uhr über jedes Lesegerät der Zutritt zum Dienstgebäude eröffnet."
> ➔I Öffentliche Verwaltung, 090600/120/2008

Sicherheit für die Beschäftigten und ihre Habe wird durch Umkleideräume und Spinde erreicht, die nur mit Beschäftigtenausweis zu öffnen sind:

> „Der Zutritt zu Umkleideräumen wird über die Spindvergabe gesteuert und muss bei der Abteilung […] beantragt werden."
> ➔I Maschinenbau, 090600/168/2013

Selten ist – wie in folgendem Beispiel – geregelt, dass Not- und Nachtausgänge nicht durch Zutrittskontrollsysteme verschlossen sein dürfen, damit das Betriebsgelände auch im Notfall und bei Ausfall des Systems verlassen werden kann:

> „An folgenden Punkten werden Kontrollmittel installiert: […] Das Drehtor als Not- bzw. Nachtausgang am […] wird mit einem Kartenleser ausgestattet. Der Ausgang ist grundsätzlich möglich und wird nicht durch eine Karte ausgelöst, der Eingang ist nur für Mitarbeiter über den Ausweis möglich."
> ➔I Ernährungsgewerbe, 090600/146/2010

2.5.3 Formen der Kontrolle

Die Auswertung zeigt: Es gibt sie noch, die reine Sichtkontrolle ohne Einsatz von technischen Systemen. Die Beschäftigten sind gefordert, die Ausweise, die dazu meist ein Lichtbild tragen, offen sichtbar zu tragen oder vorzuzeigen. Pförtner oder Sicherheitspersonal sind berechtigt, jederzeit und ohne Anlass die Identität der Person mit dem Ausweis zu vergleichen. Sie können zudem Gepäck-, Taschen- und Fahrzeugkontrollen vornehmen, um möglichen Diebstahl zu verhindern:

> „Mitarbeiterinnen, die mit einem Dienstfahrzeug oder Privatfahrzeug in das Werk einfahren, können bei der Ausfahrt aus dem Werk einer Fahrzeugkontrolle unterworfen werden."
> ➔I Fahrzeughersteller Kraftwagen, 090600/204/2012

Ausnahmen werden in diesen Fällen nur dann zugelassen, wenn das Tragen von Ausweisen ein Sicherheitsrisiko darstellt. Dies kann an bestimmten Arbeitsplätzen der Fall sein.

Die Taschenkontrollen werden beim Ausgang aus dem Unternehmen von Sicherheitspersonal vorgenommen; die Beschäftigten haben den Anweisungen Folge zu leisten. Einige Vereinbarungen begrenzen die Kontrollen mittels einer Zufallsauswahl:

> „Beim Ausgang aus dem Werk wird gleichzeitig ein Zufallsgenerator aktiviert, der das Drehkreuz sperrt, und der die Mitarbeiter/innen zu einer Taschenkontrolle aufgefordert."
> ➔I Ernährungsgewerbe, 090600/146/2010

Gemäß einer ähnlichen Vereinbarung darf nur jeder 40. von jeweils 1000 Personen kontrolliert werden.

Entsprechend verfahren einige Unternehmen bei Fahrzeugkontrollen. Diese werden ebenfalls automatisiert vorgenommen:

> „Die Kfz-Kennzeichenerkennung erfolgt durch spezielle Kameras an den Ein- und Ausfahrten des Werkes."
> ➔I Chemische Industrie, 090600/206/2012

Nachstehend ist zudem zum Schutz der Beschäftigten sichergestellt, dass die Daten anonymisiert werden:

> „Die Daten zur Kfz-Kennzeichenerkennung werden ausschließlich anonymisiert ausgewertet (Anzahl der Kfz pro Tag, Monat, Jahr), eine personenbezogene Auswertung erfolgt nicht."
> →| Chemische Industrie, 090600/206/2012

2.5.4 Grenzen der Kontrolle

Je stärker die Zutrittsrechte für Beschäftigte innerhalb des Betriebsgeländes aus Sicherheitsgründen eingeschränkt und überwacht werden, desto wichtiger ist es, dass Betriebsrat, Betriebsarzt, Personalabteilung und soziale Räume frei und unbeobachtet zugänglich bleiben:

> „Darüber hinaus haben sie Zutritt zu allgemeinen Dienstleistungsstellen des Unternehmens, speziell zu den Räumen der Personalabteilung mit Publikumsverkehr, zum Sprechzimmer des Betriebsarztes, der Kantine, des Betriebsrates etc."
> →| Maschinenbau, 090600/168/2013

Einige Vereinbarungen regeln zudem die Zutrittsrechte für Betriebsräte, Personalräte bzw. Mitarbeitervertretungen, die per Gesetz zu allen Bereichen eines Unternehmens freien Zugang besitzen. Wird dies aus Sicherheitsgründen eingeschränkt, sind spezielle Ausnahmeregelungen für die Arbeitnehmervertreter notwendig. Dies wird meist auch den Mitgliedern der Geschäftsführung und den leitenden Angestellten zugebilligt:

> „Uneingeschränkten Zutritt zum Betriebsgelände haben die Geschäftsführer, die Leitenden Angestellten und der Betriebsratsvorsitzende bzw. sein Stellvertreter."
> →| Maschinenbau, 090600/168/2013

Entsprechendes gilt für Gewerkschaftsvertreter, denen der Zutritt und Zugang zu allen Bereichen des Unternehmens bzw. der Verwaltung gemäß § 2 Abs. 2 BetrVG gewährt werden muss:

„Beauftragte von im Betrieb vertretenen Gewerkschaften erhalten zur Wahrnehmung der im Betriebsverfassungsgesetz genannten Aufgaben und Befugnisse Zutritt zum Betriebsgelände. Ist der Betriebsrat Ansprechpartner der Besucher, so kündigt der Betriebsratsvorsitzende den Besuch rechtzeitig vorher bei der Personalleitung an."

→I Maschinenbau, 090600/168/2013

2.6 Weitere Verwendung von Beschäftigtenausweisen

Wer mehr wissen möchte

Auszüge aus Vereinbarungen und Recherchemöglichkeiten zu diesem Thema finden sie hier:
http://www.boeckler.de/cps/rde/xchg/hbs/hs.xsl/4129.htm?bvdoku.theme=175#bvdoku1

Multifunktionale Beschäftigtenausweise können neben der Kontrollfunktion im Rahmen von Zugangs- und Anwesenheitskontrollen weitere Einsatzmöglichkeiten beinhalten. Die folgende Vereinbarung listet die gängigen Zwecke auf:

„Zusätzlich ermöglicht der Ausweis durch integrierte Chips eine Reihe weiterer Nutzungsmöglichkeiten. Es gelten die nachfolgend genannten Nutzungsszenarien:

- Bezahlkarte (in Kantinen, Cafeterien und an Automaten)
- Arbeitszeiterfassung (für Gleitzeitregelungen)
- Zutrittskontrolle (z. B. für Türschließsysteme)
- Zutrittserfassung (z. B. für Störfallverordnung)
- Authentifizierung (zur Anmeldung an z. B. IT-Systemen)
- Elektronische Signaturen und Zertifikate sowie Datenverschlüsselung (z. B. für sicheren elektronischen Datenversand)."

→I Branchenübergreifend, 090600/127/2009

Zusätzlich werden im Folgenden die Regelungen zum Einsatz von Beschäftigtenausweisen zur Berechtigungssteuerung für Flurförderfahrzeuge (Stapler) und für Materialausgabe-Systeme beschrieben.

Die in den vorliegenden Vereinbarungen erwähnten und eventuell geregelten Nutzungsformen von Beschäftigtenausweisen werden in diesem Kapitel beschrieben. Wenn auf andere Auswertungen von Betriebs- und Dienstvereinbarungen verwiesen werden kann, wird hier auf die Details verzichtet.

2.6.1 Digitale Signatur

Multifunktionale Ausweise werden überwiegend in Verwaltungen auch zur digitalen Signatur eingesetzt. Das Prinzip dabei ist die Authentifizierung über „Besitz und Wissen". Das heißt: Der Besitz des Ausweises ist nur in Verbindung mit dem Wissen um eine geheim zu haltende PIN geeignet, die Person eindeutig zu identifizieren. Die digitale Signatur unterliegt engen gesetzlichen Grenzen, auf die die folgende Regelung hinweist:

> „Für die Funktion der Digitalen Signatur muss die Bedienstetenchipkarte die technischen Anforderungen des Signaturgesetzes SigG und der Signaturverordnung SigV erfüllen."
> ➔ Bildungseinrichtung, 090600/181/2009

Das Signaturgesetz (SigG) und die Signaturverordnung (SigV) legen die Anforderungen an die Zertifizierungsdiensteanbieter fest. Der folgende Auszug aus einer Dienstvereinbarung beschreibt die Rahmenbedingungen sehr genau:

> „Die Einführung und Nutzung der elektronischen Signatur und anderer kryptografischer Verfahren erfordert eine Infrastruktur, die die entsprechenden Techniken und Prozesse zur Verfügung stellt. Diese Infrastruktur wird als Public Key Infrastructure (PKI) bezeichnet. Die Aufgaben, Einsatzzwecke und die Organisation der städtischen PKI sind […] beschrieben.
> CA: Certificate Authority, Zertifizierungsstelle – ordnungsgemäße Erstellung und Verwaltung von Zertifikaten
> RA: Registration Authority, Registrierungsstelle – Antragsentgegennahme, Identitätsprüfung und Ausgabe von Zertifikaten und Signaturkarten
> LRA: Lokale RA, lokale Registrierungsstelle […]
> ZRA: Zentrale RA, zentrale Registrierungsstelle […]

> Signaturkarte: (SmartCard, Chipkarte) – elektronische Speicher- und Verarbeitungseinheit zur Speicherung und Verwendung von Schlüsselpaaren […]."
> ➔ Öffentliche Verwaltung, 090600/158/2009

Die weiteren Ausführungen in dieser Vereinbarung nennen mehr Details zur sogenannten Public Key Infrastructure (PKI, → Glossar). Dies dient offenbar dazu, größtmögliche Transparenz über das Verfahren zu erreichen, damit die Beschäftigten die Beschäftigtenkarte akzeptieren.

2.6.2 Fahrzeugnutzung

Zwei der vorliegenden Vereinbarungen befassen sich mit Beschäftigtenausweisen, die zum Fahren von Flurförderfahrzeugen (FFZ, = Gabelstapler) berechtigen. Wesentlicher Regelungsinhalt ist die Datenaufzeichnung von Unfallrekordern, die in den Fahrzeugen verbaut sind:

> „Alle FFZ sind mit einem Unfallrekorder ausgestattet. Es werden unfallrelevante Betriebsdaten wie Geschwindigkeit, Lenkwinkel, Bremspedal- und Hubeinstellung etc. aufgezeichnet."
> ➔ Metallerzeugung und -bearbeitung, 090600/96/2009

Die Aufzeichnung von Daten erfolgt lediglich kurz vor und nach einer Unfallsituation, die durch Sensoren automatisch erkannt wird. Regelungsinhalt ist in beiden Vereinbarungen, dass die Auswertung der aufgezeichneten Daten so eng wie möglich begrenzt wird:

> „Die gespeicherte Transponder Nummer wird nur im Schadensfall, wenn kein Verursacher bekannt ist, zur Feststellung des letzten Benutzers ausgelesen."
> ➔ Chemische Industrie, 090600/81/2009

Die betrieblichen Vertragspartner setzen in beiden Vereinbarungen hohe Hürden (spezielle Karte, Passwortschutz) zum Zugriff auf die Unfalldaten:

> „Die Auslesekarten mit den Unfalldaten werden nur an einem PC mit Passwortschutz von berechtigten Mitarbeitenden der Stapler-

> werkstatt oder Pforte ausgelesen. Es werden die Kartennummer, Zeiten, Fahrwerte, Hubfunktionen und Fehlfunktionen des FZZ ausgelesen. Es erfolgt eine Unfallmeldung mit Schadenshöhe an das Controlling, den Betriebsrat und die Personalbetreuung. Die Personalbetreuung informiert nach Zuordnung der Kartennummer den direkten Vorgesetzten und vereinbart ein Gespräch mit dem/der Staplerfahrer/-in, der/dem Vorgesetzten und dem Betriebsrat. Die Daten werden nicht zur Leistungsmessung und zum Leistungsvergleich verwendet."
>
> ➔ Metallerzeugung und -bearbeitung, 090600/96/2009

Die zweite Vereinbarung erlaubt den Zugriff auf die Daten nur in Anwesenheit eines Betriebsratsmitglieds. Weitere Details und Textbausteine aus den Vereinbarungen sind in der Online-Datenbank enthalten.

2.6.3 Materialausgabe

Die nachstehend zitierte Regelungsabrede zu einer Testphase befasst sich mit einem Ausgabeautomaten für Verbrauchsmaterial:

> „Die Gesellschaft will den Prozess der Ausgabe von Verbrauchsmaterialien vereinfachen und optimieren. Hierzu soll ein vollautomatisiertes Ausgabesystem […] der [Firma] für ein halbes Jahr getestet werden."
>
> ➔ Maschinenbau, 091000/27/2015

Der Automat übermittelt per eingebauter UMTS-Karte die Daten an den Material-Lieferanten, sodass automatisch die notwendigen Nachlieferungen bestellt werden. Die Vereinbarung regelt, dass dabei alle Anforderungen des Datenschutzes beachtet werden:

> „Die konzernrechtlichen sowie gesetzlichen Datenschutzbestimmungen werden eingehalten."
>
> ➔ Maschinenbau, 091000/27/2015

Die Vereinbarung enthält zudem das strikte Verbot der Auswertung personenbezogener Daten:

> „Bestandsauswertungen erfolgen produkt- und artikelbezogen auf Kostenstellen, eine personenbezogene Auswertung durch Vorgesetzte, Finanzbuchhaltung, Personalabteilung oder sonstiger Stellen ist nicht gestattet."
> ➔I Maschinenbau, 091000/27/2015

Damit dürfte jegliche automatisierte Kontrolle der Beschäftigten über ihren Umgang mit Verbrauchsmaterial ausgeschlossen worden sein. Wichtig ist auch, dass die Beschäftigten ausführlich geschult werden:

> „Jeder betroffene Mitarbeiter erhält vor der Nutzung des Systems eine ausführliche Schulung durch den Betreiber bzw. durch den Betreiber geschultes internes Personal."
> ➔I Maschinenbau, 091000/27/2015

Der Inhalt der Schulungen ist jedoch nicht näher ausgeführt. Weitere Details und Textbausteine aus der Vereinbarung sind in der Online-Datenbank enthalten.

2.6.4 Zeiterfassung

Arbeitszeiterfassung und Zutrittskontrolle sind in rund einem Viertel der vorliegenden Vereinbarungen gemeinsam geregelt, da beides Funktionen einer Zeitwirtschaftssoftware sind (vgl. Kapitel 2.2.1):

> „Alle Mitarbeiter besitzen einen Chip des Zutrittskontrollsystems […], der den Mitarbeitern den Zutritt zu den verschiedenen Gebäudeteilen ermöglicht. Dieser Chip wird künftig auch für die Zeiterfassung verwendet."
> ➔I Großhandel (ohne Kfz.), 090501/201/2014

Die Zeitwirtschaftssoftware kann zudem weitere Module umfassen, beispielsweise zur Personaleinsatzplanung oder für weitere Datenerfassungen, wozu ebenfalls die Beschäftigtenausweise verwendet werden. Die betrieblichen Vertragspartner können allerdings auch übereinkommen, dass die Zeiterfassungs- oder anderweitige Funktionen ausdrücklich nicht verwendet werden sollen:

> „Die elektronische Signaturkarte wird nicht zum Zwecke der Zeiterfassung eingesetzt."
> ➔ Öffentliche Verwaltung, 090600/158/2009

Die Zeitwirtschaftsfunktionen berechnen aus den an Buchungsterminals erfassten Zeitdaten im Zusammenhang mit den Stammdaten der Beschäftigten die grundlegenden Daten für deren Entgeltabrechnung sowie für weitere Zwecke des Unternehmens:

> „Im Rahmen des Zeiterfassungssystems und der Schließanlage werden nur Daten erfasst und verarbeitet, die unmittelbar für die genannten Aufgaben notwendig sind (siehe Anlage)."
> ➔ Gesundheit und Soziales, 090600/209/2013

Details zur betrieblichen Regelung von Zeitwirtschaftssoftware sind der Auswertung von Böker (2010) zu entnehmen.

2.6.5 Bezahlfunktion

Der Beschäftigtenausweis kann in rund 15 Prozent der vorliegenden Vereinbarungen zum Bezahlen innerhalb des Unternehmens verwendet werden:

> „Der Werksausweis wird in Verbindung mit elektronischen Ausweislesern für die bargeldlose Bezahlung aller Verpflegungsleistungen auf dem Werksgelände […] verwendet. Näheres regelt Anlage […]."
> ➔ Maschinenbau, 090600/189/2013

Für den Fall, dass ein Ausweis mit Geldkartenfunktion verloren geht, enthalten die Vereinbarungen spezifische Regelungen. Üblich ist dabei, dass den Beschäftigten das Guthaben auf der Karte gutgeschrieben wird. Dies ist immer dann möglich, wenn der aktuelle Wert des Guthabens auch ohne die Karte ermittelt werden kann:

> „Bei Verlust oder Beschädigung des Ausweises wird der auf dem Ausweis gespeicherte Bargeldwert durch die Kantinenleitung ermittelt und auf eine neue Karte übertragen."
> ➔ Verlags- und Druckgewerbe, 090501/180/2013

Ist dies nicht möglich, sichern sich die Unternehmen gelegentlich im Rahmen der betrieblichen Vereinbarung gegen Schadensersatzansprüche ab:

> „Sollte der Mitarbeiterausweis als Bezahlkarte dienen, besteht bei Verlust gegen den Arbeitgeber kein Anspruch auf Auszahlung eines etwaigen Guthabens."
> ➔ Branchenübergreifend, 090600/127/2009

Mit weiteren Regelungen sind evtl. zusätzliche Details zu berücksichtigen: z. B. Benutzungsregeln für die Geldkarte, das maximale Guthaben auf der Karte oder Situationen für das Sperren von Karten. Beispiele für derartige Regelungen und Textbausteine sind in der Online-Datenbank dokumentiert.

2.6.6 Gerätenutzung und Kopierberechtigung

Eine mögliche weitere Funktion von Beschäftigtenausweisen ist die Berechtigungssteuerung bei der Benutzung von Geräten innerhalb des Unternehmens. In der folgenden Regelung wird beispielsweise die Authentifizierung bei den zentral aufgestellten Druckern über den Ausweis gesteuert. Dadurch wird eine höhere Datensicherheit erreicht: Ein Druckauftrag, der vom Arbeitsplatz an den Drucker gesendet wird, wird erst dann ausgedruckt, wenn sich die Person mit ihrer Karte am Drucker identifiziert hat:

> „Hinweis zum Transponder: Dieser dient auch der Nutzung der Follow-Me-Print-Funktion der MFP-Drucker."
> ➔ Nachrichtentechnik/Unterhaltungs-, Automobilelektronik, 090501/197/2014

Ebenso kann mittels des Beschäftigtenausweises eine Authentifizierung an anderen IT-Geräten zur Verbesserung der Sicherheit erfolgen. Einige der vorliegenden Vereinbarungen lassen diese Funktionalität zu (siehe Einleitung zu diesem Kapitel), ohne jedoch Details dazu zu vereinbaren.

2.7 Datenverwendung

Wer mehr wissen möchte
Auszüge aus Vereinbarungen und Recherchemöglichkeiten zu diesem Thema finden sie hier:
http://www.boeckler.de/cps/rde/xchg/hbs/hs.xsl/4129.htm?bvdoku.theme=175#bvdoku1

Dieses Kapitel beschreibt Regelungen, mit denen die Verwendung von Daten begrenzt, aber auch in bestimmten Fällen ausdrücklich erlaubt wird.

2.7.1 Zulässige Datenverarbeitung

Die Benutzung von Beschäftigtenausweisen führt im Zusammenhang mit technischen Erfassungsgeräten dazu, dass personenbezogene und personenbeziehbare Daten in technischen Systemen gespeichert und verarbeitet werden. Einerseits sind es die Stammdaten, mit denen die Zuordnung der Ausweise zu den Beschäftigten verwaltet werden; andererseits die Bewegungsdaten, die bei jeder Benutzung (Identifizierung) an einem Erfassungsgerät anfallen. Ein zentraler Regelungsaspekt der Vereinbarungen ist es, die Nutzung, Weitergabe und Auswertung dieser Daten zu begrenzen:

> „Die Verwendung von Zugangs- und Ausgangsdaten ist nur im Rahmen der unten genannten Zweckbestimmungen und gemäß einschlägiger Regelungen in anderen Vereinbarungen zulässig."
> →I Chemische Industrie, 090600/206/2012

2.7.2 Schnittstellen und Datenweitergabe

Schnittstellen sind Verbindungen zwischen der Software, die zur Datenverarbeitung im Zusammenhang mit den Beschäftigtenausweisen eingesetzt wird (vgl. Kapitel 2.1.4), und anderen IT-Systemen. Damit die Stammdaten von Beschäftigten nicht mehrfach in verschiedenen Softwaresystemen eingegeben werden müssen, werden sie von einem führenden System, an dem die Eingabe durchgeführt wird, an alle anderen Systeme per Schnittstelle über-

tragen. Auf diese Weise werden in der Regel auch die Stammdaten für die Ausweis- bzw. Kartenmanagementsoftware importiert:

> „Für die Mitarbeiterdaten der Konzerngesellschaften gibt es Schnittstellen zu bestehenden Personalsystemen (z. B.: […]-HR oder Konzernverzeichnisdienst), wodurch eine Übertragung von Stammdaten in das Kartenmanagementsystem erfolgt."
> ➔ Branchenübergreifend, 090600/127/2009

Schnittstellen zur Übermittlung von Daten an andere IT-Systeme – d. h. für den Export von Daten – werden in den meisten Fällen ausgeschlossen:

> „Personenbezogene Daten aus jeder der […] genannten Anwendung dürfen in keiner Form an Systeme außerhalb des Geltungsbereichs dieser Dienstvereinbarung übergeben werden."
> ➔ Bildungseinrichtung, 090600/119/2008

Für die von den betrieblichen Vertragspartnern als notwendig und zulässig erachteten Schnittstellen beschreiben die Vereinbarungen üblicherweise den Zweck der Datenübertragung und die zu übertragenden Daten. Damit soll der Missbrauch von Schnittstellen, z. B. zum Weitergeben von personenbezogenen Daten aus der Zutrittskontrolle an Auswertungssoftware, verhindert werden:

> „Die Beschreibung enthält insbesondere die Daten abgebende Stelle, die Bezeichnung und die Art der Daten, den Zweck der Übergabe und die Art der Übergabe."
> ➔ Bildungseinrichtung, 090600/119/2008

Die Daten könnten auch auf andere Weise weitergegeben werden, z. B. über Datenträger oder in gedruckter Form. Auch dazu enthalten die vorliegenden Vereinbarungen zumeist eindeutige Verbote oder verweisen auf gesetzliche Erlaubnistatbestände:

> „Sollte eine Weitergabe von personenbezogenen Daten erforderlich sein, erfolgt dies nur im Rahmen der gültigen Gesetze zum Datenschutz."
> ➔ Datenverarbeitung u. Softwareentwicklung, 090600/200/2012

2.7.3 Auswertungen

Datenauswertungen erlauben die Vereinbarungen üblicherweise nur, um die Beschäftigtenausweise zu verwalten, und nur in dem dazu notwendigen Umfang:

> „Auswertungen erfolgen lediglich im Rahmen der notwendigen Verwaltungsaktivitäten für das Kartenmanagement (z. B. Anzahl Gästekarten, Kartenstatus) durch die gemäß […] dieser Vereinbarung zuständigen Bereiche der Konzerngesellschaften. Der Umfang der Auswertungen ist auf das notwendige Maß zu begrenzen."
> ➔ Branchenübergreifend, 090600/127/2009

Zu den Verwaltungstätigkeiten gehört unter anderem die Fehlersuche nach Ausfall oder Störung des technischen Systems. Die folgende Regelung lässt dafür eine Auswertung zu und beschreibt diese – im Gegensatz zu der vorherigen, relativ offenen Regelung – sehr genau:

> „Folgende Standardauswertung (Report) mit personenbezogenen Daten von Arbeitnehmern kann erzeugt und an folgende Empfänger mit jeweils 1 Stellvertreter weitergegeben werden zur Erreichung der Zweckbestimmung:
> Reportname – Buchungsprotokoll
> Ersteller – […]
> Empfänger – […]
> Enthaltene personenbezogene Daten – Technische Fehlersuche."
> ➔ Maschinenbau, 090501/198/2013

Weitere Detailregelungen zu derlei Auswertungen enthalten die vorliegenden Vereinbarungen regelmäßig nicht.

2.7.4 Einzelfallauswertung

Sehr genau regeln die meisten Vereinbarungen, wie Daten der Beschäftigten in bestimmten Einzelfällen – zumeist strafbaren oder vertragswidrigen Handlungen von Beschäftigten – ausgewertet werden dürfen. Die folgende Regelung entstammt einer Konzernbetriebsvereinbarung:

„Bei Vorliegen dokumentierter konkreter Verdachtsmomente einer Straftat, die nicht mit Hilfe des Zutrittskontrollsystems gewonnen wurden, kann nach vorheriger Zustimmung des für den betroffenen Mitarbeiter zuständigen Standortbetriebsrates eine Auswertung der personenbezogenen Verkehrsdaten herangezogen werden, soweit andere Möglichkeiten zum Nachweis der Straftat nicht bestehen. Gleiches gilt für schwerwiegende Verstöße gegen arbeitsvertragliche Verpflichtungen. Präventive Datensuchläufe zur Auswertung personenbezogener Daten sind, gleich, ob dies heimlich oder offen geschieht, unzulässig."

→| Nachrichtentechnik/Unterhaltungs-, Automobilelektronik, 090600/174/2013

Die folgende Regelung aus einer Dienstvereinbarung erlaubt den Zugriff auf die Daten sogar nur den Strafverfolgungsbehörden. Sie regelt den weiteren Umgang mit den Daten sehr restriktiv:

„[…]

- Personenbezogene Auswertungen der Daten aus dem elektronischen Zutrittskontrollsystem sind ausschließlich für Strafverfolgungsbehörden zulässig. Der Vorgang muss bereits polizeilich zur Anzeige gebracht sein.
- Das Auslesen der Daten erfolgt durch berechtigte Administratoren (Anlage […]) unter Beteiligung des Personalrats und des Datenschutzbeauftragten. Die Weitergabe dieser Daten ist nur an die Strafverfolgungsbehörde zulässig.
- Das Auslesen darf nur dem Zwecke der Klärung der Tatsachen dienen, die als Anlass genannt wurden. Alle gewonnenen Daten, die einer solchen Klärung nicht dienlich sind, werden unverzüglich gelöscht. Die übrigen Daten sind spätestens 3 Monate nach Abschluss eines polizeilichen Ermittlungsverfahren zu löschen."

→| Bildungseinrichtung, 090600/221/2015

Das in so einem Fall anzuwendende Verfahren zur Auswertung der Daten wird auch in weiteren Vereinbarungen sehr genau beschrieben. Meist sind die Arbeitnehmervertretung und der betriebliche Datenschutzbeauftragte einbezogen. Der Zugriff auf die Daten erfolgt oft nach dem Vier-Augen-Prinzip im

Beisein eines Mitglieds der Arbeitnehmervertretung. Laut folgender Regelung wurde die Durchführung von Auswertungen auf ein sogenanntes Krisenteam übertragen und das Passwort auf die drei Parteien aufgeteilt:

> „Über eine ggf. erforderliche Auswertung der erfassten Daten entscheidet das Krisenteam bestehend aus je einem Vertreter aus dem Personalbereich, Generalsekretariat und dem Betriebsrat. Der Beschluss muss einstimmig sein. Zur Durchführung der Auswertung verfügt jede der drei Parteien über ein Drittel des Passwortes."
> →| Ernährungsgewerbe, 090600/148/2007

Nur selten darf die Geschäftsleitung oder die Leitung der Personalabteilung allein Daten auswerten, muss dann aber ein Protokoll anfertigen und damit die Arbeitnehmervertretung nachträglich unterrichten. Dies ist regelmäßig nur dann zulässig, wenn „Gefahr im Verzug" und kein Mitglied der Arbeitnehmervertretung erreichbar ist. Die folgende Regelung in einer Dienstvereinbarung bezieht zudem den betrieblichen Datenschutzbeauftragten ein:

> „Über jeden derartigen Zugriff ist ein schriftliches Protokoll anzufertigen und dem Personalrat sowie dem Datenschutzbeauftragten zu übergeben."
> →| Bildungseinrichtung, 090600/119/2008

Zur zusätzlichen Absicherung für die Beschäftigten regelt eine Vereinbarung die Beweispflicht des Arbeitgebers:

> „Im Zweifelsfall liegt die Beweispflicht dafür, dass die Informationen oder Erkenntnisse nicht missbräuchlich gewonnen wurden, bei der [Firma]."
> →| Nachrichtentechnik/Unterhaltungs-, Automobilelektronik, 090600/174/2013

2.8 Spezielle Regelungen

Wer mehr wissen möchte
Auszüge aus Vereinbarungen und Recherchemöglichkeiten zu diesem Thema finden sie hier:
http://www.boeckler.de/cps/rde/xchg/hbs/hs.xsl/4129.htm?bvdoku.theme=175#bvdoku1

Dieses abschließende Kapitel zu den Regelungsinhalten geht auf zwei spezielle Aspekte ein, die in einigen Vereinbarungen vorgefunden wurden. Es handelt sich zum einen um Regelungen zu Ausweisen für Personen, die nicht der Mitbestimmung von Arbeitnehmervertretungen unterliegen, zum anderen um Regelungen zu sehr speziellen Zutrittsbeschränkungen.

2.8.1 Besucher-Ausweise

Einige Vereinbarungen enthalten auch Regelungen zu Ausweisen, die Besuchern und Mitarbeitern von Fremdfirmen ausgehändigt werden:

> „Die Regelungen der Konzernbetriebsvereinbarung gelten in entsprechender Weise für Besucher oder Gäste sowie Beschäftigte von Fremdfirmen und sonstige Externe (nachfolgend Fremdmitarbeiter genannt), die Zutritt zu den Betriebsstätten haben."
> ➔I Branchenübergreifend, 090600/127/2009

Damit geht die Arbeitnehmervertretung allerdings über ihre formalen Regelungsbefugnisse hinaus. Diese Regelungen, die sich auf Personen beziehen, die nicht Arbeitnehmer im Sinne des BetrVG (§ 5 BetrVG) sind, entfalten keine normative Wirkung. Der Arbeitgeber ist daher nicht verpflichtet, diese Regelungen umzusetzen. Die folgende Dienstvereinbarung regelt dies vorsichtiger, die Formulierung bezieht jedoch Besucher nicht ein:

> „Die [Firma] [Stadt] wird die Regelungen dieser Dienstvereinbarung auch für die Beschäftigten anwenden, die nicht von Personalräten vertreten werden."
> ➔I Bildungseinrichtung, 090600/181/2009

2.8.2 Spezielle Zutrittsregelungen

Sicherheitsbereiche unterliegen oft sehr speziellen Zutrittsbeschränkungen. Diese sind meist als Ausnahmen zu den grundsätzlichen Regelungen in den Vereinbarungen formuliert. Wenn z. B. regelmäßig keine Daten über die Benutzung von Zutrittskontrollgeräten erfasst werden dürfen, ist dies für die Sicherheitsbereiche ausgenommen:

> „Auch bei uneingeschränktem Zutritt dürfen die besonders gesicherten Bereiche ausschließlich in Begleitung des jeweiligen Verantwortlichen bzw. entsprechend geschultem Personal betreten werden."
> ➔ Maschinenbau, 090600/168/2013

In Verbindung mit der in Kapitel 2.8.1 zuletzt zitierten Regelung ist auch hier anzumerken, dass der Geschäftsführung und den leitenden Angestellten durch diese Betriebsvereinbarung der Zutritt zu den Sicherheitsbereichen nicht verwehrt ist. Dies muss durch betriebliche Sicherheitsvorschriften außerhalb der Betriebsvereinbarung geregelt sein.

Verbindlich ist hingegen die folgende Regelung, die sich auf Betriebsräte bezieht:

> „Der Betriebsrat erhält drei Werksausweise mit Zugangsberechtigungen für alle zugangsbeschränkten Bereiche zur Verwendung durch nicht freigestellte Betriebsratsmitglieder. […] Die Ausweise der freigestellten Betriebsratsmitglieder werden für alle Bereiche frei geschaltet."
> ➔ Chemische Industrie, 090600/206/2012

Luftsicherheitsgesetz

Das Luftsicherheitsgesetz (LuftSiG) hat wesentlichen Einfluss auf einige der vorliegenden Vereinbarungen. Diese stammen aus Unternehmen, die Material per Luftfracht versenden. Sie haben Beauftragte für Sicherheit zu benennen und gesetzeskonform zu prüfen und auszubilden:

> „Der Beauftragte für Sicherheit und seine Stellvertreter haben sich einer Zuverlässigkeitsüberprüfung nach § 7 LuftSiG zu unterziehen. Dafür muss der Antrag gemäß Anlage 2 ausgefüllt werden. Die erforderliche Überprüfung und daraus folgende Beurteilung wird

> durch die zuständige Luftsicherheitsbehörde durchgeführt. […] Ist die Zuverlässigkeitsprüfung erfolgreich durchlaufen, müssen diese Personen an einer fachspezifischen Luftsicherheitsschulung teilnehmen, die von einem hierfür qualifizierten Schulungsanbieter durchgeführt wird. Die Auswahl des Schulungsanbieters und die in diesem Zusammenhang notwendigen Organisationsmaßnahmen erfolgen durch [Firma] Die Kosten der Schulung übernimmt ebenfalls [Firma]."
>
> ➔ Mess-, Steuer- und Regelungstechnik, 090600/186/2012

Zusätzlich müssen Beschäftigte, die in Sicherheitsbereichen arbeiten, einen Luftfrachtsicherheitsausweis tragen. Der Ausweis wird nach einer erfolgreich absolvierten Luftsicherheitsschulung ausgestellt. Die Ausweise in Verbindung mit Zutrittsregelungen sollen vor allem vor terroristischer Bedrohung bei dem Versand von Luftfracht schützen:

> „Die Betriebsvereinbarung beschreibt die Rahmenbedingungen für den Einsatz des Zutrittskontrollsystems. Darüber hinaus regelt diese Vereinbarung […] die gesetzeskonforme Absicherung im Sinne des Luftsicherheitsgesetzes."
>
> ➔ Nachrichtentechnik/Unterhaltungs-, Automobilelektronik, 090600/174/2013

Zusätzlich können sich Unternehmen als „Bekannter Versender" zertifizieren lassen, um Kosten durch externe Prüfungen einzusparen. Eine Vereinbarung beschreibt dies ausführlich:

> „Ohne eine Zertifizierung von [Firma] müssten die per Luftfracht zu versendenden Produkte durch Kontrollen Dritter gesichert werden. Derartige Sicherheitskontrollen nehmen zu Lasten unserer Kunden Zeit in Anspruch und werden [Firma] in Rechnung gestellt."
>
> ➔ Mess-, Steuer- und Regelungstechnik, 090600/186/2012

Die Grundlagen dazu sind im Anhang zu Artikel 2 Abs. 1 („Flughafensicherheit"), Kapitel 6.4 der EU-Verordnung 185/2010 enthalten. Darauf verweist dieselbe Vereinbarung mit der folgenden Regelung (vgl. Kapitel 2.5.1):

„Nach den gesetzlichen Bestimmungen (derzeit Verordnung VO (EG) Nr. 300/2008 vom 11. März 2008 in Verbindung mit der Verordnung VO (EU) 185/2010 vom 4. März 2010) können sich Unternehmen, die Produkte per Luftfracht sowohl in Passagier- als auch in Frachtflugzeugen versenden, in einem vom Luftfahrtbundesamt vorgeschriebenen Verfahren als ‚Bekannter Versender' zertifizieren lassen."

→| Mess-, Steuer- und Regelungstechnik, 090600/186/2012

In diesen Fällen ist der Regelungs- und Gestaltungsspielraum für die Arbeitnehmervertretung sehr gering. Im Sinne der Transparenz gegenüber den Beschäftigten ist es sicherlich hilfreich, den rechtlichen Rahmen in der Vereinbarung so ausführlich und verständlich wie möglich zu beschreiben.

3 MITBESTIMMUNGSRECHTE, -PROZEDUREN UND -INSTRUMENTE

Wer mehr wissen möchte
Auszüge aus Vereinbarungen und Recherchemöglichkeiten zu diesem Thema finden sie hier:
http://www.boeckler.de/cps/rde/xchg/hbs/hs.xsl/4129.htm?bvdoku.theme=175#bvdoku2

3.1 Mitbestimmung

Bei Einführung und Anwendung von Beschäftigtenausweisen und von technischen Systemen zu deren Anwendung für die Zutrittskontrolle und andere Zwecke ist gesetzlich und per Rechtsprechung zweifelsfrei geklärt, dass die Arbeitnehmervertretungen mitzubestimmen haben (vgl. Kapitel 6.3).

In mehreren Fällen hat die Arbeitnehmervertretung eine Rahmenvereinbarung zur IT oder Datenverarbeitung (DV) abgeschlossen, so dass die grundlegenden Rechte bereits betriebsspezifisch geregelt sind:

> „Entwicklung und Betrieb des Systems erfolgen gemäß der DV-Rahmenbetriebsvereinbarung über die Einführung und Weiterentwicklung elektronischer Datenverarbeitungssysteme in der jeweils geltenden Fassung."
> →| Chemische Industrie, 090600/206/2012

Die Vereinbarung zu Beschäftigtenausweisen in Verbindung mit einer technischen Kontrolleinrichtung kann als Zusatzvereinbarung zu dieser Rahmenvereinbarung gestaltet werden.

Teilweise werden die Vereinbarungen auf der Ebene des Konzern- oder Gesamtbetriebsrats bzw. des Haupt- oder Gesamtpersonalrats abgeschlossen. Dies ist bei einheitlicher Gestaltung und Nutzung von Beschäftigtenausweisen und den technischen Systemen sinnvoll; die Regelungskompetenz liegt gemäß Betriebsverfassungsgesetz in derartigen Fällen automatisch auf der übergreifenden Ebene. Örtliche Zusatzvereinbarungen sind dann regelmäßig

ausgeschlossen, da sie dem Ziel der Einheitlichkeit der technischen Anwendungen und der Ausweise zuwider laufen würden:

> „Im […] Konzern ist die Einführung eines einheitlichen multifunktionalen Mitarbeiterausweises vorgesehen."
> ➔I Branchenübergreifend, 090600/127/2009

Die Vereinbarungen regeln üblicherweise auch, inwieweit die Arbeitnehmervertretung bei den Änderungen der Systeme, der Verfahren oder der Zweckbestimmung mitwirken muss. Die folgende Regelung stellt ein typisches Beispiel dafür dar:

> „Wesentliche Änderungen und Erweiterungen des Zu- und Ausgangs-Kontrollsystem bedürfen der Zustimmung des Betriebsrats. Betriebsrat und Datenschutzbeauftragter werden bereits im Planungsstadium einer Änderung oder Erweiterung eingeschaltet, sodass deren Vorschläge und Bedenken im erforderlichen Maße Rechnung getragen werden kann."
> ➔I Ernährungsgewerbe, 090600/155/2011

3.2 Beteiligungsrechte

Viele Vereinbarungen sehen vor, dass die Arbeitnehmervertretung bei der – durch entsprechende Regelungen zugelassenen – Datenauswertung in Einzelfällen (vgl. Kapitel 2.7.4) zu beteiligen ist:

> „Der Betriebsrat wird über eine Nutzung der gespeicherten Daten […] rechtzeitig (innerhalb von 24 Stunden) und umfassend informiert und bei etwaigen Auswertungen im Falle bestätigter Verdachtsmomente beteiligt."
> ➔I Verlags- und Druckgewerbe, 090600/220/2015

Eine der vorliegenden Dienstvereinbarungen sieht eine regelmäßige Evaluation der Vereinbarung vor; wer diese Evaluation vornehmen soll, bleibt jedoch unklar:

> „Diese Dienstvereinbarung wird in einem Turnus, der einen Zeitraum von zwei Jahren nicht überschreiten darf, evaluiert. Sollten sich daraus Änderungen ergeben, können diese im Einvernehmen zwischen Dienststelle und Personalrat ohne Kündigung in die Dienstvereinbarung aufgenommen werden."
> ➔ Bildungseinrichtung, 050310/69/2010

Diese Maßnahme kann sinnvoll sein, um die Vereinbarung regelmäßig zu aktualisieren; sie kann möglicherweise auch die im folgenden Kapitel beschriebenen üblichen Kontrollen durch die Arbeitnehmervertretungen ersetzen.

3.3 Informations- und Kontrollrechte

Den Arbeitnehmervertretungen stehen per Gesetz umfangreiche Rechte zu, die ihnen erlauben, die eingesetzten technischen Systeme jederzeit und umfassend in Augenschein zu nehmen, sich erläutern zu lassen und deren Nutzung zu überprüfen. Auf diese Weise sollen sie feststellen können, ob die getroffenen Vereinbarungen beachtet und umgesetzt werden. Diese Rechte werden durch viele der vorliegenden Vereinbarungen bestätigt oder auch konkretisiert:

> „Der Betriebsrat behält sich das Recht vor, jederzeit innerhalb der gesetzlichen Arbeitszeit unangemeldet mit dem Datenschutzbeauftragten die Einhaltung dieser Betriebsvereinbarung sowie der datenschutzrechtlichen Bestimmungen zu kontrollieren."
> ➔ Grundstücks- und Wohnungswesen, 090600/99/2009

Um diese Rechte wahrnehmen zu können, müssen die mit den Kontrollen beauftragten Mitglieder der Arbeitnehmervertretung freien Zugang zu allen Bereichen und Räumlichkeiten des Unternehmens bekommen. Dies ist bei den durch Zutrittskontrollsysteme teilweise erheblich eingeschränkten Zutrittsrechten (vgl. Kapitel 2.5) nicht selbstverständlich, so dass es einer zusätzlichen Regelung wie in folgendem Beispiel aus einer Dienstvereinbarung bedarf:

> „Es wird sichergestellt, dass die Mitglieder des [Personalrats] einen ihrer gesetzlichen Aufgabe entsprechenden Zugang zu den Mitarbeiterinnen ihres Vertretungsbereiches haben. Dies wird mit der

> Einrichtung entsprechender Zugangsberechtigungen für die Mitglieder des [Personalrats] sichergestellt, die ihnen freien Zugang zu allen Gebäuden und Bereichen (nicht einzelnen Räumen) ermöglichen, für die keine speziellen Sicherheitsanforderungen (z. B. Rechenzentrum, […] Laborbereiche) definiert sind."
> →I Gesundheit und Soziales, 090600/90/2007

Als Grundlage für Kontrollen regeln einige Vereinbarungen, dass ausführliche Systembeschreibungen zu der eingesetzten Technik und zu den Beschäftigtenausweisen als Anlage der Vereinbarung hinzugefügt werden oder zumindest jederzeit von der Arbeitnehmervertretung eingesehen werden können:

> „Die verantwortliche Stelle ist verpflichtet, dem Betriebsrat oder der mit der Überprüfung beauftragten Person sämtliche für die Überprüfung benötigten Unterlagen zur Verfügung zu stellen und die für Prüfzwecke erforderlichen Auskünfte zu geben."
> →I Mess-, Steuer- und Regelungstechnik, 090600/201/2013

Einige Arbeitnehmervertretungen erhalten regelmäßig Informationen über die Nutzung der Beschäftigtenausweise bzw. der technischen Systeme:

> „Der Betriebsrat erhält einmal im Monat eine Aufstellung über die aktuellen Daten."
> →I Metallerzeugung und -bearbeitung, 090600/96/2009

Um welche Daten es sich hierbei handelt, und ob bzw. inwieweit diese Daten anonymisiert sind, bleibt bei dieser Regelung offen. Andere Vereinbarungen regeln genauer, dass beispielsweise die vergebenen Zugriffsrechte, die Systemprotokolle oder die erstellten Auswertungen bzw. Statistiken eingesehen werden können und ggf. zu erläutern sind.

Wenn bei den Kontrollen Abweichungen von den Regelungen der Betriebs- bzw. Dienstvereinbarung festgestellt werden, verlangen einzelne Vereinbarungen die umgehende Beseitigung dieser Mängel:

> „Bei der Ausübung dieses Kontrollrechtes ggf. festgestellte Mängel sind umgehend abzustellen."
> →I Branchenübergreifend, 090600/127/2009

Falls es keine derartigen Regelungen gibt, kann man davon ausgehen, dass die Arbeitnehmervertretung im jeweiligen gesetzlichen Rahmen handeln wird.

Damit die Arbeitnehmervertreter ihre Kontrollaufgaben wahrnehmen können, benötigen sie entweder einen (internen oder externen) Sachverständigen oder sie müssen ausreichend dafür qualifiziert sein. Regelungen zur Hinzuziehung externer Sachverständiger finden sich in den vorliegenden Vereinbarungen nicht. Hingegen findet man in einigen Dienstvereinbarungen Regelungen zu dem Recht, an speziellen Schulungsmaßnahmen teilzunehmen:

> „Mitglieder der Personalräte sind berechtigt, zur Wahrnehmung ihrer Aufgaben aus dieser Vereinbarung an Weiterbildungsveranstaltungen zu den hier geregelten Themen teilzunehmen. Die Kosten trägt die Dienststelle."
> ➔I Bildungseinrichtung, 090600/181/2009

3.4 Konfliktregelungen

Konflikte entstehen im Zusammenhang mit Beschäftigtenausweisen und Kontrolltechniken einerseits dadurch, dass die Beschäftigten die Ausweise nicht regelungskonform anwenden; andererseits dadurch, dass die Arbeitgeber Kontrollen durchführen oder dies zumindest beabsichtigen, die gemäß Vereinbarung nicht zulässig sind.

Zu Konflikten mit den Beschäftigten ist es übliche Regelungspraxis, dass ein Verfahren zur Konfliktlösung beschrieben und dass die Arbeitnehmervertretung einbezogen wird. In der Regel ist in diesen Konfliktsituationen eine Auswertung der gespeicherten Daten vorgesehen, wie es auch die folgende Regelung beschreibt (vgl. Kapitel 2.7.4):

> „Über eine ggf. erforderliche Auswertung der erfassten Daten entscheidet das Krisenteam, bestehend aus je einem Vertreter aus dem Personalbereich, Werkschutzleitung und dem Betriebsrat."
> ➔I Ernährungsgewerbe, 090600/155/2011

Ist ein Fehlverhalten des Arbeitgebers der Auslöser eines Konflikts, wird in den meisten Fällen nicht erst eine innerbetriebliche Problemlösung angestrebt, sondern sofort die Einigungsstelle angerufen:

> „Bei allen Streitigkeiten, die aus dieser Betriebsvereinbarung entstehen, kann die [Firma] oder der Betriebsrat die Einigungsstelle gern § 76 BetrVG anrufen."
>
> ➔| Kreditgewerbe, 090600/188/2013

Eine Dienstvereinbarung regelt sehr weitgehend, dass bei Verletzung von Datenschutz und Datensicherheit das technische System außer Betrieb genommen werden muss:

> „Die Dienststelle ist verpflichtet, […]-Anwendungssysteme ganz oder teilweise außer Betrieb zu nehmen, wenn sich herausstellt, dass Datensicherheit und Datenschutz im Sinne dieser Dienstvereinbarung nicht gewährleistet sind. Der Personalrat kann dies in begründeten Fällen auch verlangen."
>
> ➔| Bildungseinrichtung, 090600/119/2008

4 OFFENE PROBLEME

Dieses Kapitel verweist auf Auffälligkeiten, problematische Regelungen und möglicherweise fehlende Regelungsinhalte in den vorliegenden Vereinbarungen.

Rund ein Drittel der vorliegenden Vereinbarungen sind Dienstvereinbarungen aus öffentlichen Verwaltungen und Bildungseinrichtungen wie z. B. Hochschulen. Diese Vereinbarungen sind regelmäßig wesentlich umfangreicher und enthalten mehr detaillierte Regelungen als die meisten Betriebsvereinbarungen. Dienstvereinbarungen beschreiben häufig sehr genau das Aussehen der Beschäftigtenausweise, die darin gespeicherten Daten, die Vorgänge bei der Benutzung der Ausweise und die Verfahrensweisen der technischen Systeme. Zudem enthalten die Dienstvereinbarungen häufig die Verfahrensweisen zur Benutzung der Ausweise im Sinne eines Manuals. Insgesamt wird dadurch die Transparenz gegenüber den Beschäftigten in den Vordergrund der Regelungen gestellt.

Bei vielen Betriebsvereinbarungen zu Beschäftigtenausweisen und -kontrollen wird nicht deutlich: Kommen sie den Mitarbeiterinnen und Mitarbeitern zugute? Wenn ja: in welchem Umfang? In welcher Form? Teilweise regeln die Vereinbarungen offenbar nur einen Teil des technischen Systems: beispielsweise wenn sie nur die Ausgabe und Verwendung von Beschäftigtenausweisen, nicht aber die weiteren technischen Details und die Benutzung des Zutrittskontrollsystems regeln. Der mögliche Missbrauch der Systeme ist damit nicht gänzlich ausgeschlossen. Oft werden in den Vereinbarungen noch nicht einmal der Hersteller und die Bezeichnung des Softwaresystems genannt. Dies eröffnet dem Arbeitgeber die Möglichkeit, das System ohne Änderung der Vereinbarung und eventuell ohne Zustimmung des Betriebsrats auszutauschen.

In diesem und in anderen Fällen wäre zu prüfen, ob die Vereinbarungen einer rechtlichen Prüfung standhalten würden. So ist beispielsweise nicht eindeutig geklärt: Inwieweit können in Betriebs- bzw. Dienstvereinbarungen verbindliche Regelungen getroffen werden zur Verwendung von Beschäftigtenausweisen für Besucher oder für andere Personen, die nicht der Mitbestimmung unterliegen? Offenbar werden die Vereinbarungen zu Beschäftigtenausweisen und deren Nutzung für die Zutrittskontrolle oder für andere Zwecke überwiegend ohne Hinzuziehung technischer Sachverständiger und ohne juristische Prüfung abgeschlossen. Darauf deuten teilweise auch For-

mulierungen hin, die jede nötige Klarheit vermissen lassen oder schlicht und einfach bedeutungslos sind. Einige betriebliche Verhandlungspartner regeln beispielsweise die Zeiterfassung, die Dienstplanung, die Zutrittskontrolle und die Nutzung von Beschäftigtenausweisen für andere Zwecke in einer einzigen Vereinbarung. Das mag sinnvoll erscheinen, wenn alle diese Funktionen über ein einziges technisches System realisiert werden. In einigen ausgewerteten Vereinbarungen führt dies jedoch dazu, dass die einzelnen Regelungsgebiete nur unzureichend berücksichtigt sind. Empfehlenswert wäre daher, die jeweilige Anwendung ausführlich zu vereinbaren und dadurch ggf. für ein technisches System mehrere Vereinbarungen abzuschließen, die jeweils ein Modul bzw. einen abgegrenzten Funktionsbereich umfassen.

5 ZUSAMMENFASSENDE BEWERTUNG

Moderne multifunktionale Beschäftigtenausweise bieten sowohl für Unternehmer als auch für ihre Beschäftigten Vorteile gegenüber herkömmlichen Arten zur Identifizierung und Authentifizierung: Höhere Sicherheit und besserer Komfort lassen eine „win-win"-Situation entstehen. An den ausgewerteten Vereinbarungen ist zu erkennen, dass die Arbeitnehmervertretungen deswegen der Einführung von elektronischen Ausweisen sowie maßvollen Kontrollen grundsätzlich positiv gegenüberstehen.

Die Vereinbarungen verweisen auf den zunehmenden Schutzbedarf gegen äußere und innere Bedrohungen aus Sicht der Unternehmen. Die Ausweise in den unterschiedlichen Arten und Ausprägungen werden zu den jeweils als notwendig und sinnvoll erachteten Kontrollen eingesetzt. Mit den Regelungen treffen die betrieblichen Vertragspartner die jeweils angemessen erscheinende Abwägung zwischen dem Sicherheitsbedarf und dem Persönlichkeitsschutz der Beschäftigten.

In den meisten Dienstvereinbarungen aus Stadtverwaltungen, Universitäten und anderen öffentlichen Einrichtungen stehen die Vorteile der Anwendung multifunktionaler Ausweise und genaue Verfahrensregelungen zur Verwendung und Verwaltung der Ausweise im Vordergrund. Darin unterscheiden sich die Dienstvereinbarungen in erheblichem Maße von den Betriebsvereinbarungen. Ob und inwieweit sich Regelungsziele und -inhalte von Betriebs- und Dienstvereinbarungen im Laufe der Zeit angenähert haben, konnte nicht festgestellt werden.

Das Sicherheitsbewusstsein scheint allgemein größer zu werden. Viele Verantwortliche in Unternehmen und Verwaltungen fühlen sich bzw. das von ihnen zu schützende Gut offenbar zunehmend Bedrohungen ausgesetzt, auf mehreren Ebenen: seien es Terrorangriffe, Brandanschläge und andere Gefahren von außen wie Angriffe „von innen", aus den Reihen der Beschäftigten. Je unpersönlicher die Organisationen werden, desto größer wird das Misstrauen gegenüber dem Einzelnen. Neben dem Materiellen sind insbesondere auch das unternehmensinterne Wissen und Know-how sowie die IT-Infrastruktur immer wieder vor Angriffen zu schützen.

Damit korrespondierend verzeichnen die Hersteller von Sicherheitstechnik und -software große Auftragszuwächse, soweit dies den Messen, Internetauftritten und Veröffentlichungen zu entnehmen ist. Sie bieten zudem immer neue Sicherheitstechnik, -verfahren und -methoden an. Mit dem Sicherheits-

argument wird die IT-Technik permanent vorangetrieben und verfeinert, seien es Zutrittskontrollen, Zeiterfassung, Internetzugänge etc. Aufgrund der generellen Zustimmung der Beschäftigten zu der Verwendung von Ausweis- und Kontrollsystemen können die Arbeitnehmervertreter oft wenig mehr als einen minimalen Schutz der Persönlichkeitsrechte erzielen – dies lassen jedenfalls die vorliegenden Vereinbarungen erkennen. Den gesetzlichen Anforderungen (BetrVG, BDSG etc.) wird zwar noch Rechnung getragen; doch die Regelungen über Ausnahmen zum bestehenden Schutz der Persönlichkeitsrechte der Beschäftigten überwiegen. Dies wird insbesondere bei Regelungen zu Einzelfallauswertungen erkennbar, die teilweise nur geringe Hürden aufweisen. Ein weiteres Indiz ist die oft nachlässig beschriebene Technik der Systeme, die aufgrund fehlender Regelungen im Detail missbräuchlich genutzt werden kann (vgl. Kapitel 4).

Wer die innerbetrieblichen Verhandlungen zu derartigen Vereinbarungen kennt, weiß, wie schwierig es oft ist, den Persönlichkeitsschutz der Beschäftigten hochzuhalten und ihn dem Schutz des Eigentums des Unternehmens gleichzustellen. „Der Schutz von Beschäftigten vor zu viel Kontrolle und die Verhinderung von Missbrauch und Straftaten durch zu wenig Kontrolle stehen in einem starken Spannungsverhältnis.“ (Maschke/Werner 2015, Seite 8)

Das Datenschutz-ignorierende Verhalten von Beschäftigten in ihrem Privatleben einerseits und die offenbar stetig steigenden extremistischen Bedrohungen sind aus Arbeitgebersicht jene Argumente, mit denen sich alle betrieblichen Sicherheits-, Kontroll- und Überwachungsmechanismen und -techniken begründen und durchsetzen lassen. Der von Maschke/Werner 2015 diagnostizierte Trend zur Vereinbarung von Mitbestimmungsrechten, die über die gesetzlichen Möglichkeiten hinausgehen, lässt sich in den ausgewerteten Vereinbarungen nicht gleichermaßen feststellen.

6 BERATUNGS- UND GESTALTUNGSHINWEISE

Dieses Kapitel gibt in kompakter Form Anregungen, welche Punkte bei der Mitgestaltung wichtig sein könnten. Das Ziel der Veröffentlichung, vorliegende betriebliche Regelungen zu analysieren und dabei einen Überblick über verbreitete Praktiken zu geben, erlaubt es nicht, allzu sehr in die Einzelheiten zu gehen. Die zahlreichen Hinweise sind in folgendem Gestaltungsraster zusammengefasst. Es handelt sich dabei nicht um einen geschlossenen Vorschlag zur unmittelbaren Anwendung, sondern um einen Stichwortkatalog zur Unterstützung eigener Überlegungen. Es ist ein Angebot, sich mögliche Regelungspunkte einer Vereinbarung noch einmal im Überblick zu verdeutlichen, um die zentralen Aspekte für die eigene Situation zu finden.

6.1 Gestaltungsraster

Ausweise und Technik

- System-Komponenten vollständig und abschließend in einer Anlage zur Vereinbarung dokumentieren
  - Ausweiskarte, Transponder etc., möglichst mit Abbildungen
  - Systembestandteile (Hardware, Software etc.)
- Datenarten vollständig und abschließend in einer Anlage zur Vereinbarung benennen
  - Systemdaten (Netzwerksoftware, Betriebssystem, Programmdateien)
  - Berechtigungsdaten (Identifikationsnummern, Berechtigungen, Benutzer)
  - Ereignisdaten (personen-, orts- und zeitabhängige Daten der Ausweisnutzung, Protokolldateien)
- Zweckbestimmung der Daten, Speicherort und Speicherdauer vereinbaren

Verfahrensregelungen

- Ausweisverwaltung: alle zulässigen Prozesse beschreiben
  - Herstellung, Individualisierung, Ausgabe an Beschäftigte, Rücknahme, sonstige Verwaltungsaufgaben, Besonderheiten
- Beschäftigte: alle Rechte und Pflichten beschreiben
  - Empfang durch Beschäftigte, Rückgabe, Verwendung, Benutzungspflicht, Tragepflicht, Besonderheiten

- Störfälle: vollständige Darstellung aller möglichen Störfälle und deren Folgen
  - technische Defekte, Verlust, Vergessen, Beschädigung, Kosten für Ausweisersatz, Beweispflicht

Rechte der Beschäftigten

- Wahrung der Persönlichkeitsrechte, Datenschutz, auch Recht am eigenen Bild; Lichtbild nur für Ausweis verwendbar
- Informationsrechte für Beschäftigte gemäß Datenschutzgesetz zusichern und konkretisieren; Recht auf Einweisung und Schulung im erforderlichen Umfang
- Einverständniserklärungen, falls notwendig, als Anlage zur Vereinbarung dokumentieren
- Freiwilligkeit der Nutzung von Beschäftigtenausweisen vereinbaren, falls möglich
- Gleichbehandlung der Beschäftigten vereinbaren, sofern realisierbar, ansonsten Unterschiede mit Begründung definieren

Verwendung der Beschäftigtenausweise für Zutritts- und Anwesenheitskontrollen

- Kontrollzwecke möglichst konkret benennen, z. B. Unternehmenssicherung, Beschäftigtensicherheit, dabei das Gefährdungspotenzial beschreiben, evtl. auf Gefährdungsanalysen und/oder externe Anforderungen verweisen, z. B. Luftsicherheitsgesetz, Zertifizierung etc.
- Kontrollbereiche festlegen, z. B. Betriebsgelände, Gebäude, Etagen, Räume
- Formen der Kontrolle, z. B. Sichtkontrolle, Taschen- und Gepäckkontrolle, Fahrzeugkontrolle, Kfz-Kennzeichenkontrolle) auf das erforderliche Maß begrenzen, Zufallsauswahl mit eindeutiger Bestimmung, eindeutige Regeln für die zur Kontrolle Berechtigten
- spezielle Zutrittsregelungen, ggf. ohne Protokollierung und Kontrollmöglichkeiten konkret beschreiben und begründen, z. B. uneingeschränkte Zutrittsregelungen für Arbeitnehmervertreter, Gewerkschaftsvertreter, Datenschutzbeauftragte, Sicherheitsbeauftragte etc.; spezielle Zutrittsregeln für Sicherheits- und Gefahrenbereiche

Weitere Verwendung von Beschäftigtenausweisen

- mögliche Verwendungsarten in Vereinbarungen regeln (Digitale Signatur, Zeiterfassung, Bezahlfunktion, Identifikation für Fahrzeugnutzung, Materialausgabe, Gerätenutzung oder Kopierberechtigung)

- Regelungen zur Ausweisverwendung durch Besucher, Gäste, Leitende Angestellte, Fremdmitarbeiter etc. grundsätzlich nicht in die Vereinbarung aufnehmen; eigenständige freiwillige Vereinbarung mit dem Arbeitgeber treffen

Datenverwendung

- zulässige Verarbeitung der gespeicherten und durch Ausweisnutzung erhobenen Daten (Stammdaten, Bewegungsdaten) auf das Notwendigste begrenzen (Datenminimalität) und zu allen Daten den Erhebungs- und Verarbeitungszweck (als Anlage zur Vereinbarung) dokumentieren
- Schnittstellen, Datenweitergabe grundsätzlich untersagen, zulässige Schnittstellen nur mit eindeutigem Zweck erlauben, Liste der zulässigen Schnittstellen mit genauer Beschreibung und Empfänger als Anlage zur Vereinbarung
- Auswertungen nur zu statistischen Zwecken in anonymisierter Form zulassen, personenbezogene oder -beziehbare Auswertungen nur mit eindeutigem Zweck erlauben, Liste der zulässigen Auswertungen mit genauer Beschreibung und Empfänger als Anlage zur Vereinbarung
- Einzelfall-Auswertungen nur in sehr begrenztem Rahmen bei konkretem Verdacht auf Straftaten und unter Beteiligung der Arbeitnehmervertretung, ggf. nur für externe Strafverfolgungsbehörden zulassen
- Datenschutzbeauftragte einbeziehen, Aufgaben und Rechte regeln
- Aufbewahrungs-/Löschfristen eindeutig mit Verweis auf rechtliche Grundlagen festlegen
- Verbot der Leistungs- und Verhaltenskontrolle, Verbot der Erstellung von Bewegungsprofilen
- Berechtigungen und Zugriffsregelungen aufgabenbezogen und minimal
- Fernzugriff begrenzen und protokollieren

Rechte der Arbeitnehmervertretung

- Mitbestimmung bei jeder Veränderung, die sich auf die Vereinbarung auswirken könnte
- Beteiligung bei Einzelfallauswertungen
- Recht auf Information über jede Veränderung in Bezug zur Vereinbarung
- angemessene Kontrollrechte, um die Einhaltung der Vereinbarung überprüfen zu können, u. a. Zugriff auf Systemprotokolle, Dokumentationen, ggf. Hinzuziehung interner und externer Sachverständiger

Konfliktregelungen, Verfahrensweisen
- bei Konflikten zwischen Beschäftigten und Arbeitgeber
- bei Konflikten zur Vereinbarung, sofern vom gesetzlichen Weg (z. B. Einigungsstelle gemäß § 76 BetrVG) abgewichen werden soll.

6.2 Ausgangspunkte für die gestaltende Einflussnahme durch die Interessenvertretung

Dieses Kapitel wiederholt nicht sämtliche bisher behandelten Gesichtspunkte. Stattdessen liefert es Anregungen für eine Positionsbestimmung der Arbeitnehmervertretung bei der Regelung von Beschäftigtenausweisen, Zugangskontrollsystemen und weiteren technischen Einrichtungen, die Ausweise zur Identifikation und Authentifizierung verwenden.

Beschäftigtenausweise und Zugangskontrollen können heutzutage von Beschäftigten und ihren Vertretungen weitgehend als akzeptiert angesehen werden. Die Verwendung von Ausweisen zur Identifikation ist allgemein als notwendiges Sicherheitssystem, das auch dem Schutz der Beschäftigten dient, anerkannt. Gleichzeitig bleibt jedoch die Sorge vor Missbrauch durch den Arbeitgeber („Profilbildung") und durch Externe, so dass Datenschutz und Datensicherheit ausführlich zu regeln sind.

Vor Einführung von Beschäftigtenausweisen, Zugangskontrollsystemen etc. ist es wichtig, dass der Betriebs- bzw. Personalrat einen möglichst objektiven Standpunkt entwickelt. Die Durchführung einer Sicherheits- bzw. Gefährdungsanalyse ist angebracht. Das Datenschutzrecht verlangt eine Abwägung mit den schutzwürdigen Interessen der Beschäftigten. Rechtliche und andere externe Vorschriften zur Unternehmenssicherheit sind eingehend zu analysieren; teilweise versuchen die Arbeitgeber mit dem Hinweis auf Gesetze oder Zertifizierungen mehr als vorgeschrieben Beschäftigtendaten zu erheben, zu verarbeiten, auszuwerten und langfristig aufzubewahren.

Ist die Entscheidung gefallen, Beschäftigtenausweise einzuführen, stellt sich vorrangig die Frage nach den technischen Systemen, die mit den Ausweisen bedient werden müssen. Diese Systeme erheben, speichern und verarbeiten personenbezogene Daten. Der eigentliche Verwendungszweck ist dabei in der Regel eingeschränkt. Eine Datensammlung auf Vorrat und beliebige Auswertungen sind durch die Datenschutzgesetze untersagt. Die Umsetzung der gesetzlichen Anforderung nach Datenminimalität ist in den betrieblichen Vereinbarungen so konkret zu beschreiben, dass kein Interpretationsspielraum bleibt.

Die Betriebs- bzw. Dienstvereinbarung zu Beschäftigtenausweisen sollte sich abgestimmt in den betrieblichen Regelungsbestand einfügen. Es handelt sich hierbei einerseits um eine Vereinbarung zu einer technischen Einrichtung; andererseits um eine Vereinbarung zur Ordnung im Betrieb (vgl. Kapitel 6.3). Diese sollte sich in evtl. bestehende Rahmenvereinbarungen nahtlos einordnen und zu diesen nicht im Widerspruch stehen. Gelegentlich orientieren sich die Vereinbarungen an Regelungen zu einem früheren Ausweis- oder Zugangskontrollsystem, das durch die aktuelle Vereinbarung abgelöst wird. Da jedoch zwischen beiden Vereinbarungen oft viele Jahre liegen, sind die betrieblichen Bedingungen, denen sich die neue Vereinbarung anzupassen hat, vermutlich stark verändert. Dies gilt es beim Verfassen der neuen Regelungsinhalte dringend zur berücksichtigen.

6.3 Wesentliche rechtliche Grundlagen

Das BetrVG gibt den Betriebsräten das Mitbestimmungsrecht bei Einführung und Anwendung von Systemen, die zur Kontrolle von Leistung und Verhalten der Beschäftigten geeignet sind (§ 87 Abs. 1 Nr. 6 BetrVG). Dies lässt keine Zweifel daran aufkommen, dass die Einführung und Anwendung von Beschäftigtenausweisen im Zusammenhang mit einem Zugangskontrollsystem oder einer anderen der in dieser Auswertung genannten technischen Systeme mitbestimmungspflichtig sind. In jedem Fall werden die Ausweise personalisiert und ihre Anwendung wird personenbezogen dokumentiert, so dass Rückschlüsse auf das Verhalten der Person möglich sind.

Doch auch die Einführung von Beschäftigtenausweisen, die nicht zur technischen Erfassung angewendet werden, sondern lediglich zur Sichtkontrolle getragen werden müssen, unterliegt der Mitbestimmung durch den Betriebsrat. Die gesetzliche Grundlage dafür bietet § 87 Abs. 1 Nr. 1 BetrVG. Bei der Einführung und Anwendung dieser Ausweise handelt es sich um eine Frage der Ordnung des Betriebs und des Verhaltens der Arbeitnehmer im Betrieb. Werden einheitliche Ausweise für alle Beschäftigten eines auf mehrere Standorte verteilten Unternehmens oder gar eines Konzerns eingeführt, so ist der Gesamt- bzw. Konzernbetriebsrat zuständig.

Beschäftigtenausweise, die für leitende Angestellte, Besucher oder Fremdfirmenmitarbeiter ausgestellt werden, unterliegen nicht der Mitbestimmung des Betriebsrats. Trotzdem finden sich in einigen ausgewerteten Vereinbarungen spezielle Regelungen für diesen Personenkreis oder es wird darauf hingewiesen, dass die Vereinbarung auch für diese Personen anzuwenden ist.

Da es sich hierbei jedoch nicht um einen mitbestimmungspflichtigen Tatbestand handelt, sind derartige Regelungen auf freiwilliger Basis entstanden. Dies hat ggf. Auswirkungen auf die Nachwirkung bei Kündigung der Vereinbarung. Sofern keine anders lautenden Regelungen getroffen wurden, entfalten die freiwilligen betrieblichen Vereinbarungen keine Nachwirkung.

Vergleichbare Rechte gelten für Personalräte in Einrichtungen des Bundes gemäß BPersVG und in Landeseinrichtungen der meisten Bundesländer gemäß jeweiligem LPersVG sowie für Mitarbeitervertretungen in Einrichtungen der Kirchen. Bei der Ausarbeitung von Betriebs- bzw. Dienstvereinbarungen zu Beschäftigtenausweisen ist insbesondere das jeweils anzuwendende Bundes-, Landes- oder kirchliche Datenschutzgesetz zu beachten.

7 BESTAND DER VEREINBARUNGEN

Tabelle 1: Art und Anzahl der Vereinbarungen

Art der Vereinbarung	Anzahl
Konzern-Betriebsvereinbarung	2
Gesamt-Betriebsvereinbarung	1
Rahmenbetriebsvereinbarung	1
Betriebsvereinbarung	27
Rahmendienstvereinbarung	1
Dienstvereinbarung	13
Regelungsabrede	1
gesamt	**46**

Tabelle 2: Verteilung der Vereinbarungen nach Branchen

Branchen	Anzahl
Bergbau	1
Bildungseinrichtung	7
branchenübergreifend	1
chemische Industrie	3
Datenverarbeitung und Softwareentwicklung	2
Ernährungsgewerbe	3
Fahrzeughersteller Kraftwagen	1
Gesundheit und Soziales	5
Großhandel (ohne Kfz.)	1
Grundstücks- und Wohnungswesen	1
Kirchen	1
Kohlebergbau	1
Kreditgewerbe	2
Maschinenbau	5
Mess-, Steuer- und Regelungstechnik	2

Branchen	Anzahl
Metallerzeugung und -bearbeitung	1
Nachrichtentechnik/Unterhaltungs-, Automobilelektronik	2
öffentliche Verwaltung	4
unternehmensbezogene Dienstleistungen	1
Verlags- und Druckgewerbe	2
Gesamt	**46**

Tabelle 3: Abschlussjahr der Vereinbarungen

Abschlussjahr	Anzahl
2007	2
2008	3
2009	8
2010	2
2011	4
2012	4
2013	16
2014	2
2015	5
gesamt	**46**

GLOSSAR

LEGIC advant
„LEGIC“ ist die Bezeichnung für eine Technologie zur Entwicklung von ID-Systemen. Seit 2002 wird die Technologieplattform von der gleichnamigen Schweizer Aktiengesellschaft über lizenzierte Partnerunternehmen vertrieben und in unterschiedlichsten Anwendungen zur Identifikation verwendet. „advant“ bezeichnet eine moderne Form dieser Technologie für die spezielle Anwendung in Transpondern.

MIFARE DESFire
„MIFARE“ ist eine weit verbreitete Technik für berührungslos arbeitende Chipkarten. „DESFire“ ist eine aktuelle, sicherheitsoptimierte Ausprägung dieser Technik für Zugangskontroll- und Zeiterfassungssysteme.

PLUS-Zweigstellen von Kreditinstituten
Geschäftsstellen von Kreditinstituten mit sogenannten „Beschäftigtenbedienten Banknotenautomaten“ (BBA-Stellen) werden auch PLUS-Stellen genannt.

Public Key Infrastructure (PKI)
Gesamtsystem (Infrastruktur) zum Ausstellen, Verteilen und Prüfen von digitalen Zertifikaten als Grundlage für elektronische Unterschriften unter Verwendung von asymmetrischer Verschlüsselung.

Radio-Frequency Identification (RFID)
Identifizierung von Objekten mit Hilfe elektromagnetischer Wellen; Bezeichnung für eine Technologie zum berührungslosen und automatischen Identifizieren und Lokalisieren der mit entsprechenden Funketiketten ausgestatteten Gegenstände oder Lebewesen aller Art mittels Radiowellen.

LITERATUR- UND INTERNETVERZEICHNIS

Böker, Karl-Hermann (2009): Videoüberwachung, Reihe Betriebs- und Dienstvereinbarungen/ Kurzauswertungen, Hans-Böckler-Stiftung (Hg.), Düsseldorf, Download: http://www.boeckler.de/pdf/mbf_bvd_videoueberwachung.pdf, Abruf am 16.01.2017.

Böker, Karl-Hermann (2010): Zeitwirtschaftssysteme, Betriebs- und Dienstvereinbarungen, Hans-Böckler-Stiftung (Hg.), Frankfurt am Main; Download: http://www.boeckler.de/pdf/mbf_bvd_zeitwirtschaftssysteme.pdf, Abruf am 16.01.2017.

Maschke, Manuela/Werner, Nils (2015): Arbeiten 4.0 – Diskurs und Praxis in Betriebsvereinbarungen, Mitbestimmungsförderung/Report Nr. 14, Oktober 2015, 1. Fassung, Düsseldorf, Download: http://www.boeckler.de/pdf/p_mbf_report_2015_14.pdf, Abruf am 16.01.2017.

Internethinweise
Im Geheimschutzhandbuch (GHB) definiert das Bundesministerium für Wirtschaft und Energie (BMWi) die für den Geheimschutz in der Wirtschaft konkret erforderlichen Maßnahmen und Regeln zum Zugang zu Verschlusssachen: www.bmwi-sicherheitsforum.de/handbuch, Abruf am 30.01.2017

ÜBER DIE SAMMLUNG VON BETRIEBSVEREINBARUNGEN

Die Hans-Böckler-Stiftung verfügt über die bundesweit einzige bedeutsame Sammlung betrieblicher Vereinbarungen, die zwischen Unternehmensleitungen und Belegschaftsvertretungen abgeschlossen werden. Derzeit enthält unsere Datenbank etwa 16.000 Vereinbarungen zu ausgewählten betrieblichen Gestaltungsfeldern.

Unsere breite Materialgrundlage erlaubt Analysen zu betrieblichen Gestaltungspolitiken und ermöglicht Aussagen zu Trendentwicklungen der Arbeitsbeziehungen in deutschen Betrieben. Regelmäßig werten wir betriebliche Vereinbarungen in einzelnen Gebieten aus. Leitende Fragen dieser Analysen sind: Wie haben die Akteure die wichtigsten Aspekte geregelt? Welche Anregungen geben die Vereinbarungen für die Praxis? Wie ändern sich Prozeduren und Instrumente der Mitbestimmung? Existieren ungelöste Probleme und offene Fragen? Die Analysen betrieblicher Vereinbarungen zeigen, welche Regelungsweisen und -verfahren in Betrieben bestehen. Die Auswertungen verfolgen dabei nicht das Ziel, Vereinbarungen zu bewerten, denn die Hintergründe und Strukturen in den Betrieben und Verwaltungen sind uns nicht bekannt. Ziel ist es, betriebliche Regelungspraxis abzubilden, Trends aufzuzeigen und Gestaltungshinweise zu geben.

Bei Auswertungen und Zitaten aus Vereinbarungen wird streng auf Anonymität geachtet. Die Kodierung am Ende eines Zitats bezeichnet den Standort der Vereinbarung in unserem Archiv und das Jahr des Abschlusses. Zum Originaltext der Vereinbarungen haben nur Mitarbeiterinnen und Mitarbeiter des Archivs und Autorinnen und Autoren Zugang.

Zusätzlich zu diesen Auswertungen werden vielfältige anonymisierte Auszüge aus den Vereinbarungen in der Online-Datenbank im Internetauftritt der Hans-Böckler-Stiftung zusammengestellt. Damit bieten wir anschauliche Einblicke in die Regelungspraxis, um eigene Vorgehensweisen und Formulierungen anzuregen.

Das Internetangebot ist unmittelbar zu erreichen unter
www.boeckler.de/betriebsvereinbarungen

Anfragen und Rückmeldungen richten Sie bitte an
betriebsvereinbarung@boeckler.de

Multifunktionale Ausweise für Beschäftigte sind heute eher die Regel, nicht die Ausnahme. Diese Auswertung befasst sich mit Regelungen zu Beschäftigtenausweisen, Zutrittskontrollen sowie zur Kontrolle von Gepäck und Fahrzeugen auf dem Firmengelände. 46 aktuelle betriebliche Vereinbarungen wurden ausgewertet.
Sicherheitsanforderungen wachsen, in vielen Branchen werden verstärkt Kontrollen durchgeführt. Beispiele zeigen wesentliche Regelungsgegenstände und erleichtern die Gestaltung eigener Betriebs- und Dienstvereinbarungen.

WWW.BOECKLER.DE

ISBN 978-3-86593-264-8