TELETRUST Deutschland e. V.
Verein zur Förderung der Vertrauenswürdigkeit von Informations- und Kommunikationstechnik

www.teletrust.de

Orientierungshilfe für eine Betriebsvereinbarung beim Einsatz biometrischer Systeme

Arbeitsgruppe 6 „Biometrische Identifikationsverfahren“

AK „Rechtliche Aspekte der Biometrie“

Version: 1.2
Status: final
Datum: 21.09.2005
Edition: Dr. Astrid Albrecht, BSI

Dieses Dokument ist entstanden durch die aktive Mitarbeit von:

Dr. Astrid Albrecht, Bundesamt für Sicherheit in der Informationstechnik
Dr. Manfred Bromba, Bromba GmbH Biometrics
Dr. Gerrit Hornung, LL.M., Projektgruppe verfassungsverträgliche Technikgestaltung (provet), Universität Kassel
Dr. Gunter Laßmann, T-Systems
Dr. Gisela Quiring-Kock, Der Hessische Datenschutzbeauftragte

Externe Beratung:
Rechtsanwalt Achim Thannheiser, Hannover

Weitere AG 6-Mitglieder haben qualitätssichernd mitgewirkt.

TeleTrusT Deutschland e.V.
Chamissostraße 11
99096 Erfurt

A. Einleitung

Nach den Regelungen des Betriebsverfassungsgesetzes[1] unterliegt die betriebliche Einführung eines biometrischen Systems[2] der Mitbestimmung des Betriebsrats[3]. Dieses Mitbestimmungsrecht umzusetzen ist Sinn und Zweck einer Betriebsvereinbarung. Die von der AG 6 "Biometrische Identifikationsverfahren" des TeleTrusT e.V. erarbeitete Orientierungshilfe soll als Vorschlag dienen und dazu beitragen, die wesentlichen Aspekte bei der Erstellung und Verhandlung mit dem Arbeitgeber[4] zu beachten.

Auch für solche Unternehmen, bei denen kein Betriebsrat und/oder betrieblicher Datenschutzbeauftragter etabliert ist, ist die Berücksichtigung der im Folgenden dargelegten Grundsätze zu empfehlen, um einerseits die berechtigten Interessen des Arbeitgebers sowie andererseits die schutzwürdigen Belange der Beschäftigten angemessen gegeneinander abzuwägen. Darüber hinaus sollte auch in solchen Fällen ein Verantwortlicher im Betrieb benannt werden, der auf der einen Seite die Persönlichkeitsrechte der Beschäftigen zu wahren sucht und auf der anderen Seite Ansprechpartner für den Arbeitgeber in allen wesentlichen Belangen bzgl. der Einführung des biometrischen Systems sein kann.

Um eine bessere Lesbarkeit und Handhabbarkeit zu erreichen, wurden nähere Erläuterungen und Anmerkungen in Form von Fußnoten am Ende des Textes eingefügt, die die konkrete Umsetzung und Anwendung in der Praxis erleichtern sollen[5].

B. Planung und Pilotierung

Um das Bedürfnis des Arbeitgebers zur Einführung des biometrischen Systems begründen zu können, ist eine Pilotierung des einzusetzenden Systems unter Einbeziehung des Betriebsrats sowie des betrieblichen Datenschutzbeauftragten (bzw. eines anderen Verantwortlichen, s.o.) zu empfehlen, und zwar im Vorfeld des Abschlusses der Betriebsvereinbarung. Gegebenenfalls empfiehlt sich hierfür der Abschluss einer gesonderten Betriebsvereinbarung.

Durch das Pilotierungsprojekt im Vorfeld soll der Arbeitgeber nachweisen, dass der Ersatz des ggfs. bisher verwendeten Verfahrens durch den Einsatz biometrischer Systeme erforderlich und begründet ist und das biometrische System nachweislich für den definierten Zweck praxistauglich ist[6]. Am leichtesten wird ihm dies bei einem entsprechenden Sicherheitsbedürfnis fallen. Daneben kommt der Einsatz eines biometrischen Systems auch aus Gründen der besseren Bedienbarkeit (im Vergleich zu herkömmlichen Methoden) und des dadurch möglichen höheren Benutzungskomforts sowie der Kosteneinsparung in Betracht. Wegen des Eingriffs in das Recht auf informationelle Selbstbestimmung ist in jedem Fall ein berechtigtes Interesse des Arbeitgebers notwendig. Eine Verwendung personenbezogener Daten ist stets dann erforderlich, wenn diese ein geeignetes Mittel zur Erreichung des angestrebten Zwecks ist, für das es keine sinnvolle und zumutbare Alternative gibt[7]. Dies sollte durch den Arbeitgeber frühzeitig dargelegt und im Austausch mit den benannten Stellen im Betrieb diskutiert werden. Dabei ist auch Umfang und Dauer der Pilotphase festzulegen sowie die Verantwortlichen für die informationstechnische Umsetzung bereits einzubeziehen.

Um die Akzeptanz des betrieblichen biometrischen Systems bei den Beschäftigten zu gewährleisten, soll der Betriebsrat bzw. ein anderer Verantwortlicher bereits in der Planungs- und Pilotierungsphase eingebunden werden. Gegenüber den Beschäftigten ist durch den Arbeitgeber für die erforderliche Transparenz bezüglich der Datenerhebung, -verarbeitung und -nutzung der biometrischen Daten zu sorgen. Dabei wird er aktiv vom Betriebsrat unterstützt. Der betriebliche Datenschutzbeauftragte ist ebenfalls von Beginn an eingebunden und wirkt auf die Einhaltung des Schutzes der in diesem Zusammenhang verarbeiteten und genutzten Daten der Beschäftigten hin.

Die benannten Stellen im Betrieb sind zudem in die Auswahl des biometrischen Systems eingebunden und in solchem Umfang zu schulen, dass sie das System und seine datenschutzgerechte Funktionsweise qualifiziert beurteilen können, um anschließend bei dessen Einführung und dem Abschluss der Betriebsvereinbarung kompetent mitbestimmen zu können. Der Projektbericht sollte, jedenfalls in der Zusammenfassung, auch den Beschäftigten zur Verfügung gestellt werden.

Schließlich sollte vorher geregelt werden, welche Maßnahmen ergriffen werden sollen, wenn die Pilotierungsphase zu einem negativen Ergebnis kommt und der Testverlauf zeigt, dass das avisierte biometrische System nicht zur Erfüllung des angestrebten Zwecks geeignet ist.

C. Betriebsvereinbarung (Muster)

Zwischen der Geschäftsleitung der Firma ……. und dem Betriebsrat der Firma ……. über den betrieblichen Einsatz biometrischer Systeme im Rahmen von Zutritts- / Anwesenheits- / Verweildauer-kontrolle oder Zugangs- / Zugriffssicherung (bzw. andere Anwendungsgebiete)[8].

I. Präambel[9]

Bei der vorliegenden Betriebsvereinbarung handelt es sich um eine Einigung über den betrieblichen Einsatz biometrischer Systeme zur Wahrung der Interessen des Arbeitgebers auf der einen und der Persönlichkeitsrechte der Beschäftigten[10] auf der anderen Seite. Die Vertragspartner sind sich dabei darüber einig, dass es sich bei den zu erfassenden biometrischen Daten um personenbezogene Daten handelt, die als solche im Sinne des Datenschutzes behandelt werden müssen. Diese Betriebsvereinbarung stellt eine Rechtsgrundlage im Sinne von § 4 I BDSG zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten dar und schafft damit eine eigenständige Eingriffsgrundlage[11].

II. Allgemeines

1. Gegenstand[12]

Diese Betriebsvereinbarung regelt die Einführung, den Einsatz, die Nutzung und die Nutzungsänderung biometrischer Systeme und die dabei erfolgende Weiterverarbeitung biometrischer Daten, die von der ……. [Firma] genutzt werden, unabhängig vom Standort dieser Systeme.

2. Geltungsbereich

Die Betriebsvereinbarung gilt für alle Beschäftigten des Unternehmens und in Bezug auf sämtliche im Arbeitsbereich der Beschäftigten zum Einsatz kommenden biometrischen Systeme, wobei es keine Rolle spielt, wo sich diese Systeme befinden[13].

2a. Bei Entsendung in fremde Firmen

Die in dieser Betriebsvereinbarung festgelegten Regelungen zum Einsatz biometrischer Systeme gelten auch für Mitarbeiter der ……. [Firma], die in einem Fremdunternehmen eingesetzt werden, das ebenfalls biometrische Systeme verwendet. Es besteht Einigkeit zwischen den Vertragspartnern, dass dem Mitbestimmungsrecht des Betriebsrates nicht entgegensteht, dass das biometrische System im Kundenbetrieb und nicht im eigenen Betrieb eingerichtet ist[14]. Sollte dies nicht möglich sein, so wird der Arbeitgeber dafür Sorge tragen, dass eine Erfassung biometrischer Daten von Beschäftigten bei Drittunternehmen nicht erfolgt.

3. Geltungsdauer

Diese Betriebsvereinbarung gilt ab dem Zeitpunkt des Zustandekommens auf unbestimmte Dauer.

Alternative:

Diese Betriebsvereinbarung gilt ab ..... bis .....[15]. Eine Nachwirkung wird ausgeschlossen.

III. Inhaltliche Regelungen

1. Ziele und Gründe des Einsatzes biometrischer Verfahren[16]

Beim bisher im Betrieb eingesetzten Zutrittskontrollverfahren[17] haben sich in der Vergangenheit einige, die Sicherheit des Betriebs gefährdenden und damit wesentlichen Sicherheitsmängel gezeigt. Betriebsinterne Untersuchungen haben ergeben, dass ...[18]. Aus diesem Grund ist es wegen des berechtigten Sicherheitsbedürfnisses des Arbeitgebers notwendig, ein alternatives Zutrittskontrollverfahren einzusetzen. Das geplante biometrische System verspricht die Befriedigung dieses Bedürfnisses unter gleichzeitiger Wahrung der Persönlichkeitsrechte der Arbeitnehmer[19].

Ziel des Einsatzes des biometrischen Systems ist es, die betriebliche Zutrittskontrolle sicherer zu gestalten. Die Pilotierungsphase hat gezeigt, dass System XY dieser Anforderung genügt. Im Rahmen der Pilotierung konnte eine Falschzurückweisungsrate von (Beispiel) unter 1 % bei einer Falscherkennungsrate von ebenfalls unter 1 % erreicht werden. Damit kann sichergestellt werden, dass bei grundsätzlich gleichbleibender Sicherheit des Zutritts nur eine geringe Anzahl von Berechtigten vom System abgewiesen werden. Die Verfügbarkeit des Systems sowie die Benutzbarkeit durch die Arbeitnehmer hat sich über die Pilotierungsphase stabil erwiesen[20]. Bei der vertraglichen Gestaltung mit dem Anbieter wurde eine werktägliche Supportleistungen vor Ort vereinbart, um Systemausfälle und andere Störungen ohne Beeinträchtigung der das System benutzenden Beschäftigten im Arbeitsablauf zu gewährleisten sowie die hinreichende Schulung der internen Mitarbeiter, die das System im Haus betreuen und warten.

2. Einführungsphase

Die Einführung des biometrischen Systems erfolgt unter umfassender Information der Beschäftigten und wird aktiv sowohl vom Betriebsrat als auch vom betrieblichen Datenschutzbeauftragten bzw. einem weiteren Verantwortlichen begleitet. Der Arbeitgeber stellt sicher, dass diese Stellen alle für die Beurteilung des biometrischen Systems notwendigen Informationen zur Verfügung haben. Diese sind in verständlicher Form an die Beschäftigten vor der Einführung weiterzugeben.

Den Beschäftigten werden bereits bei der Erstregistrierung (Enrollment) alle Informationen über das biometrische System und den Umgang des Arbeitgebers mit den biometrischen Daten zur ständigen Verfügung entweder im Intranet des Betriebs oder offline in einer Broschüre zur Verfügung gestellt[21]. Um die möglichst reibungslose Verwendung des biometrischen Systems durch die Beschäftigten sicherzustellen, werden alle Nutzer in einer einmaligen durch den Arbeitgeber zu organisierenden Informationsveranstaltung über die Betriebsweise des Systems und deren Benutzung informiert. Ferner ist sicherzustellen, dass die Beschäftigten im Umgang mit dem biometrischen System und dem Enrollment hinreichend geschult werden. Wird das Enrollment nicht durch den Anbieter des biometrischen Systems durchgeführt, stellt der Arbeitgeber sicher, dass die das Enrollment durchführenden Personen selbst rechtzeitig vorab entsprechend geschult werden. Zu diesem Zweck werden die betroffenen Beschäftigten von ihrer sonstigen Arbeit temporär freigestellt.

Schließlich wird durch den Arbeitgeber ein ständig verfügbarer Ansprechpartner benannt, der bei Fragen, Problemen, Anregungen oder Hinweisen der Beschäftigten während der regelmäßigen Arbeitszeit zur Verfügung steht. Hierbei ist sicherzustellen, dass derartige Anfragen nur in anonymisierter Form weiter gegeben und vertraulich behandelt werden. Entweder im Intranet -soweit allen Beschäftigten ohne weiteres zugänglich- und/oder offline wird zudem ein "Kummerkasten" bereitgestellt, um den Beschäftigten, die sich nicht persönlich an diesen Ansprechpartner wenden möchten, eine entsprechende Möglichkeit der Äußerung zu geben.

Wenn aufgrund technischer Probleme die Offenlegung der Identität eines Beschäftigten erforderlich ist, wird durch geeignete Vorkehrungen sichergestellt, dass die Persönlichkeitsrechte des betroffenen Beschäftigten gewahrt werden und eine Weitergabe der persönlichen Daten nicht erfolgt. Eine über die reine Behebung der Funktionsstörung hinausgehende personenbezogene Auswertung von Problemfällen oder eine weitergehende Verwendung dieser Daten ist unzulässig. Der Arbeitgeber stellt sicher, dass auch in technischer Hinsicht geeignete Vorkehrungen getroffen werden, damit zusätzliche Auswertungen bereits von vornherein ausgeschlossen sind.

3. Transparenz

Um die Akzeptanz des biometrischen Systems in der betrieblichen Praxis zu erhöhen, ist eine umfassende Transparenz über das biometrische System, seine Funktionsweise und die Erhebung, Speicherung und Verarbeitung der biometrischen Daten zu gewährleisten. Zu diesem Zweck ist eine laufende Information der Arbeitnehmer über die genannten Aspekte vor und während der Einführungsphase sowie während des laufenden Betriebs vorzunehmen[22]. Ferner sind FAQ (Häufig gestellte Fragen und Antworten) -Listen einzurichten, mit Hilfe derer sich die Beschäftigten bei Problemen oder Fragen zusätzlich informieren können. Der Arbeitgeber stellt sicher, dass sowohl die Informationen als auch die FAQ-Listen stets auf dem aktuellen Stand gehalten werden. Schließlich sind Mitglieder der Arbeitnehmervertretung sowie der betriebliche Datenschutzbeauftragte bzw. der weitere Verantwortliche laufend in die biometrische Anwendung einzubinden und im notwendigen Umfang zu qualifizieren.

4. Diskriminierungsfreier Einsatz - Ersatzverfahren

Um einen diskriminierungsfreien Einsatz des biometrischen Systems zu gewährleisten, ist ein Ersatzsystem zur Verfügung zu stellen, das für solche Arbeitnehmer vorgehalten wird, die über das betreffende biometrische Merkmal nicht oder nicht in der notwendigen Ausprägung verfügen. Trotz Sicherstellung einer möglichst geringen Fehlenrollmentrate während der Pilotierung kann nicht ausgeschlossen werden, dass es derartige "Fehlnutzer" in der Arbeitnehmerschaft gibt. Um diese vor Diskriminierungen zu schützen, ist die Vorhaltung des Ersatzsystems erforderlich[23]. Über das vorzuhaltende Ersatzsystem entscheidet der Arbeitgeber mit dem Betriebsrat unter Einbeziehung des betrieblichen Datenschutzbeauftragten[24]. Der Arbeitgeber stellt sicher, dass den betroffenen Fehlnutzern keine Nachteile welcher Natur auch immer aus der Nicht-Nutzung des biometrischen Systems entstehen[25].

5. Sicherheitsaspekte

Die Pilotierung hat ein besonderes Augenmerk auf die Erkennungsleistung und Sicherheit des biometrischen Systems geworfen und Fehlerraten von *xyz* ergeben, die sowohl aus Sicht der Sicherheit als auch hinsichtlich des Nutzerkomforts von beiden Parteien als akzeptabel angesehen werden[26]. Das einzusetzende biometrische System verfügt darüber hinaus über eine Lebenderkennung, deren Funktionstüchtigkeit ebenfalls während der Pilotierung bestätigt wurde[27]. Eine Risikoanalyse, die u.a. Angriffsszenarien untersucht und mögliche Gegenmaßnahmen aufzeigt wird unter Einbeziehung des TeleTrusT-Kriterienkatalogs und der besonderen Fachkunde des *A-Instituts* erstellt[28]. Diese Analyse ist vom Arbeitgeber in Auftrag zu geben und dem Betriebsrat, dem betrieblichen Datenschutzbeauftragten bzw. dem anderen Verantwortlichen (s. oben unter 2.) zur Verfügung zu stellen.

6. Datenschutz

Das jeweils anzuwendende Bundes- (BDSG) bzw. Landesdatenschutzgesetz ist einzuhalten[29]. Der Arbeitgeber stellt sicher und ist dafür verantwortlich, dass das einschlägige Datenschutzgesetz von allen Führungskräften und Arbeitnehmern sowie externen Stellen eingehalten wird.

a. Zweckbindung

Die biometrischen Daten der Arbeitnehmer werden nur für Zwecke der Zutrittskontrolle[30] erhoben, verarbeitet und genutzt[31]. Eine Weitergabe in nicht anonymisierter Form an Dritte oder auch andere Unternehmensbereiche ist unzulässig. Ein Einsichtsrecht besteht nur für die zuständigen Beschäftigten in der Personalabteilung und die Systemadministratoren, die vorab auf ihre Verschwiegenheitspflichten zu verpflichten sind. Es findet keine Leistungs- oder Verhaltenskontrolle unter Verwendung der biometrischen Daten statt.

Bei einer gesetzlich erlaubten Zweckänderung[32] ist der Arbeitgeber für die rechtmäßige Herausgabe der betroffenen Daten verantwortlich. Er hat Betriebsrat sowie betrieblichen Datenschutzbeauftragten unverzüglich von der Anfrage auf Herausgabe zu unterrichten und mit diesen gemeinsam über den Umfang der Herausgabe zu beraten.

b. Datenerhebung und -speicherung

Das biometrische System wird im Verifikationsmodus[33] betrieben. Eine zentrale Datenbank mit den biometrischen Daten aller Arbeitnehmer wird nicht eingerichtet[34]. Die Referenzdaten sind vielmehr auf einem mobilen Speichermedium (Token) wie z.B. einer Chipkarte gespeichert, der sich im Besitz des jeweiligen Arbeitnehmers befindet[35].

c. Datenvermeidung und Datensparsamkeit

Es werden lediglich die Daten erhoben und gespeichert, die für die eigentliche Erkennung auch tatsächlich notwendig sind[36].

Bereits bei der Wahl des biometrischen Systems ist darauf zu achten, dass möglichst keine Überschussinformationen (z.B. über den Gesundheitszustand) anfallen. Das technische System ist zudem so zu gestalten, dass es z.B. eine Bewegungsverfolgung nicht ermöglicht, wenn sie nicht zwingend erforderlich ist.

Die erfassten Daten werden weiterhin auf ein Minimum reduziert und verschlüsselt[37]. Falls trotzdem ein Informationsüberschuss entsteht, wird eine weitergehende Verwendung ausgeschlossen.

Sowohl Datenvermeidung und -sparsamkeit als auch die Auswahl des konkreten biometrischen Verfahrens sowie die Gestaltung des Systems sind Gegenstand der Vorabkontrolle (vgl. z.B. §4d Abs. 5 BDSG, §7 Abs. 6 HDSG), die je nach anzuwendendem Recht unterschiedlich ausgestaltet ist[38].

d. Datenschutzaudit

Der Arbeitgeber verpflichtet sich, ein Datenschutzaudit nach § 9a BDSG durchzuführen[39].

e. Löschungsfristen

Nach Ausscheiden eines Arbeitnehmers aus der Firma oder nach Abschaffung der biometrischen Systeme sind die entsprechenden biometrischen Daten vollständig und unwiederbringlich zu löschen bzw. das Speichermedium zu vernichten.

7. Technische und organisatorische Maßnahmen[40]

Der Arbeitgeber hat die wirksame Umsetzung der nach § 9 und Anlage zu § 9 BDSG bzw. dem entsprechenden Landesdatenschutzgesetz erforderlichen technischen und organisatorischen Maßnahmen sicherzustellen und zu dokumentieren. Die Dokumentation ist dem Betriebsrat und dem betrieblichen Datenschutzbeauftragten zur Verfügung zu stellen. Bei identifiziertem Änderungsbedarf hat der Arbeitgeber sicherzustellen, dass die Änderungen im Datenschutz und -sicherheitskonzept zügig umgesetzt werden. Der Betriebsrat hat in Zusammenarbeit mit dem betrieblichen Datenschutzbeauftragten über die Einhaltung der genannten Anforderungen zu wachen, Mängel aufzuzeigen sowie auf deren Beseitigung hinzuwirken.

a. Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen die biometrischen Daten verarbeitet oder genutzt werden, durch den Arbeitgeber zu verwehren.

b. Zugangskontrolle

Der Arbeitgeber stellt sicher, dass die Datenverarbeitungssysteme nicht von Unbefugten genutzt werden können.

c. Zugriffskontrolle

Die zur Benutzung eines Datenverarbeitungssystems Berechtigten dürfen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Es wird zudem vom Arbeitgeber sichergestellt, dass biometrische Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

d. Weitergabekontrolle:

Zu gewährleisten hat der Arbeitgeber weiterhin, dass biometrische Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Zudem ist durch geeignete Maßnahmen wie z.B. eine revisionssichere Protokollierung zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen diese personenbezogenen Daten übermittelt werden.

e. Auftragskontrolle:

Biometrische Daten, die im Auftrag verarbeitet werden, dürfen nur entsprechend den Weisungen des Auftragsgebers verarbeitet werden[41].

f. Verfügbarkeitskontrolle:

Die biometrischen Daten müssen gegen zufällige Zerstörung oder Verlust geschützt werden.

8. Evaluierung

Es findet eine regelmäßige, mindestens jährliche Überprüfung der Eignung des eingesetzten biometrischen Systems statt[42]. Eine Überprüfung erfolgt darüber hinaus bei wesentlichen Änderungen sowie im Fall besonderer Vorkommnisse wie z.B. bekannt gewordener Missbrauchsfälle. Die Überprüfung wird durch Vertreter des Arbeitgebers und des Betriebsrats, durch den Datenschutzbeauftragten sowie einen Vertreter der IT-Abteilung durchgeführt sowie das Ergebnis dokumentiert. Die Beschäftigten werden über die Evaluierung in Kenntnis gesetzt.

9. Wiederherstellung des ursprünglichen Zustands

Bei erkennbarer Nicht-Eignung des biometrischen Systems zu dem vorab definierten Zweck sollte bei unverzüglich durchgeführter erfolgloser technischer Verbesserung des Systems die vollständige Wiederherstellung des ursprünglichen Zustands erfolgen. Die Nicht-Eignung des Systems ist im Rahmen der genannten Evaluierung festzustellen[43].

10. Rechte der Beschäftigten

Jeder Mitarbeiter hat das Recht, sich während der Arbeitszeit über diese Betriebsvereinbarung zu informieren und hierzu Fragen zu stellen. Der Arbeitgeber ist verpflichtet, innerhalb einer angemessenen Frist auf diese zu antworten, bzw. einen geeigneten Ansprechpartner damit zu beauftragen. Den Beschäftigten sind u.a. Informationen über den Speicherungsumfang und – den Ort mit der Einführung des Systems zuzuleiten.

IV. Schlussvorschriften

1. Verfahren bei Streitigkeiten

Bei allen Streitigkeiten, die aus dieser Betriebsvereinbarung entstehen, kann die [Firma] oder der Betriebsrat die Einigungsstelle gem. § 76 BetrVG anrufen. Die Parteien unterwerfen sich bereits jetzt dem Spruch der Einigungsstelle.

2. Verstöße gegen die Betriebsvereinbarung

Verstöße gegen die in dieser Betriebsvereinbarung aufgestellten Regelungen sind entsprechend zu sanktionieren[44].

3. Salvatorische Klausel

Sollte eine Bestimmung dieser Betriebsvereinbarung unwirksam sein, wird die Wirksamkeit der übrigen Bestimmungen davon nicht berührt. Die Parteien verpflichten sich, anstelle einer unwirksamen Bestimmung eine dieser Bestimmung möglichst nahe kommende Regelung zu treffen. Meinungsverschiedenheiten und Unklarheiten im Zusammenhang mit dieser Betriebsvereinbarung werden im Übrigen zwischen den Vertragsparteien um Sinne einer vertrauensvollen, konstruktiven und respektvollen Zusammenarbeit entschieden.

4. Inkrafttreten, Kündigung

Diese Vereinbarung tritt am …… in Kraft und kann mit einer Frist von drei Monaten zum Jahresschluss, erstmals zum …… gekündigt werden[45]. Ist diese Betriebsvereinbarung wirksam gekündigt, verliert sie ihre Bedeutung als Rechtsgrundlage im Sinne von § 4 Absatz 1 BDSG[46]. Die Parteien schließen ausdrücklich eine Nachwirkung i. S. d. § 77 Abs. 6 BetrVG aus.

Mit der Beendigung dieser Betriebsvereinbarung und bei Fehlen einer Neuregelung ist das biometrische System außer Betrieb zu stellen. Dabei ist sicherzustellen, dass alle im Zusammenhang mit dem Betrieb angefallenen personenbezogenen Daten unwiederbringlich gelöscht werden.

D. Literaturhinweise/Materialien (Auswahl)

Albrecht, Astrid, Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, Hrsg.: Prof. Dr. Dr. h.c. Spiros Simitis, Nomos 2003, insbesondere S. 195 ff. zu Persönlichkeitsschutz der Arbeitnehmer beim betrieblichen Einsatz biometrischer Systeme

Albrecht, Astrid, Biometrie zum Nutzen für Verbraucher? (in: Datenschutz und Datensicherheit 2000, S.332 ff.)

Albrecht, Astrid, Mitbestimmungsrecht des Betriebsrates (in: Datenschutz und Datensicherheit 2000, S. 361)

Albrecht, Astrid und *Probst, Thomas,* Biometrie für alle? (in: Datenschutz und Datensicherheit 2000, S.318)

Arbeitsgericht Frankfurt a. M., Beschluss vom 18. Februar 2002 – 15 BVGa 32/02

Art. 29 Arbeitsgruppe, Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten, Arbeitspapier 5062/01/DE (WP 48) vom 13.09.2001

Bäumler, H., Biometrie datenschutzgerecht gestalten - Die Bedeutung von Technikgestaltung für den Datenschutz, (in: Datenschutz und Datensicherheit 1999, S. 128)

Böker, Karl-Hermann und *Kübeck, Horst,* Biometrische Systeme zur Zeiterfassung und Zutrittskontrolle (in: Computer-Fachwissen 6/2004, S.8 ff.)

Bundesarbeitsgerichtsbeschluss vom 27. Januar 2004 – 1 ABR 7/03 – http://juris.bundesarbeitsgericht.de/cgi-bin/rechtsprechung/document.py?Gericht=bag&Art=pm&Datum=2004&Sort=3&anz=4&pos=1&nr=9420

Büllingen, Franz und *Hillebrand, Annette,* Biometrie als Teil der Sicherungsinfrastruktur? (in: Datenschutz und Datensicherheit 2000, S.339 ff.)

Gola/Schomerus, BDSG, 7. Auflage 2002

Gundermann, L./Probst, Th., Brennpunkte des Datenschutzes, Kapitel 9 (in: Roßnagel, A.: Handbuch des Datenschutzrechts, C.H. Beck München 2003)

Hornung, Gerrit, Der Personenbezug biometrischer Daten (in: Datenschutz und Datensicherheit 2004, S.429 ff.)

Hornung, Gerrit / Steidle, Roland, Biometrie am Arbeitsplatz - sichere Kontrollverfahren versus ausuferndes Kontrollpotential" ist, Arbeit und Recht (AuR) 2005, 201 ff.

Saeltzer, Gerhard, Sind diese Daten personenbezogen oder nicht? (in: Datenschutz und Datensicherheit 2004, S.218 ff.)

Simitis, Spiros, BDSG, Kommentar, 5. Auflage 2003

Weichert, Th., Biometrie - Freund oder Feind des Datenschutzes, (in: Computer und Recht (CR) 1997, S. 369 ff.)

E. Hinweise und Anmerkungen

1

Im Folgenden werden insbesondere die betriebsverfassungsrechtlichen Aspekte beleuchtet und daher auch vom "betrieblichen" Einsatz biometrischer Systeme gesprochen. Für entsprechende Dienstvereinbarungen im öffentlichen Bereich gilt das jeweils einschlägige Personalvertretungsrecht.

2

Ein betrieblicher Einsatz biometrischer Systeme kommt für unterschiedliche Bereiche in Betracht: Zutrittskontrollen am Betriebseingang oder zu bestimmten Sicherheitsbereichen, das Single-Sign-On an PC-Arbeitsplätzen (Zugangskontrolle zu bestimmten Daten), die Sicherung von Speichermedien wie etwa USB-Sticks, die Absicherung der Authentizität von Handlungen der Beschäftigten bei elektronischen Signaturen etc.

3

Es handelt sich bei einem biometrischen System regelmäßig um eine technische Einrichtung, die gemäß § 87 I Nr. 6 BetrVG die zur Überwachung des Verhaltens der Arbeitnehmer bestimmt ist (bzw. § 75 III Nr. 17 BPersVG). Dies gilt auch, wenn das biometrische System lediglich als Zutrittskontrolle eingesetzt werden und tatsächlich nicht der Überwachung dienen soll. Denn die Vorschrift ist so auszulegen, dass die Möglichkeit der Überwachung ausreicht (BAG v. 9.9.1975 und 14.9.1984 in AP Nr. 2, 9 zu § 87 BetrVG Überwachung) Sofern biometrische Systeme als Zugangskontrollsystem dienen, greift nach der Rechtsprechung des BAG (27.01.2004, 1 ABR 7/03, AP Nr. 40 zu § 87 BetrVG Überwachung) ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 1und Nr. 6 BetrVG ein (anders jedoch das BAG zu allgemeinen anonymen Zugangskontrollen 10.4.1984, AP Nr. 7 zu § 87 BetrVG 1972 Überwachung). Danach hat der Betriebsrat auch mitzubestimmen in Fragen der Ordnung des Betriebs (§ 87 Abs. 1 Nr. 1 BetrVG) und des Verhaltens der Arbeitnehmer im Betrieb. Wo die erfassten Daten ausgewertet und ob sie überhaupt ausgewertet werden, ist dabei ohne Belang. Sinn des Mitbestimmungsrechts ist es nämlich, die Beschäftigten vorbeugend zu schützen (so schon das BAG vom 9. 9. 1975 – 1 ABR 20/74 – AP Nr. 2 zu § 87 BetrVG 1972, ›Überwachung‹). Das Betriebsverfassungsgesetz konkretisiert letztlich nur den datenschutzrechtlichen Persönlichkeitsschutz, wonach jeder wissen darf und muss, wer mit welchen seiner Daten was und wo macht. Dieses so genannte ›informationelle Selbstbestimmungsrecht‹ geht auf die Rechtsprechung des Bundesverfassungsgerichts von 1983 zurück und wird seither vom BAG angewendet (vgl. BAG vom 14.9.1984 – 1 ABR 23/82 – AP Nr. 9 zu § 87 BetrVG 1972, ›Überwachung‹). Aus diesem Gedanken heraus können biometrische Systeme auch unzulässig sein, wenn der Anwendungsbereich und die Verletzung der Persönlichkeitsrechte im obigen Sinne unverhältnismäßig sind.

4

Es wird nachfolgend versucht geschlechtsneutral zu formulieren. Dies ist nicht immer möglich. Zur besseren Lesbarkeit wird dann die althergebrachte männliche Form verwendet, ohne dass damit das weibliche Geschlecht herabgesetzt oder ausgeschlossen werden soll.

5

Grundsätzlich -abgesehen von weiteren Initiativrechten und dem Einigungsstellenverfahren- gilt:

Wenn ein Betriebsrat der Meinung ist, eine Betriebsvereinbarung abschließen zu wollen oder zu müssen, muss er hierüber einen ordentlichen Beschluss fassen, vgl. §§ 29, 33 und 34 BetrVG. Der Arbeitgeber wird dann aufgefordert, entsprechende Verhandlungen aufzunehmen. Es empfiehlt sich, bereits zu diesem Zeitpunkt einen Entwurf der beabsichtigten Betriebsvereinbarung zu präsentieren. Kommt es in der Folge zu einer Einigung mit dem Arbeitgeber, muss der Betriebsrat wiederum in einem ordentlichen Beschluss auf einer Betriebsratssitzung über den Inhalt und Abschluss der Betriebsvereinbarung beschließen. Nach § 77 Absatz 2 BetrVG sind Betriebsvereinbarungen schriftlich niederzulegen. Im Falle einer Einigung zwischen Arbeitgeber und Betriebsrat sind sie von jeweils einer vertretungsberechtigten Person der beiden Parteien (Betriebsrat: idR der Vorsitzende) zu unterschreiben.

Der Betriebsrat muss zuvor einen Beschluss fassen, mit dem er den Betriebsratsvorsitzenden ermächtigt, stellvertretend für den Betriebsrat die Betriebsvereinbarung abzuschließen.

6

Andererseits bedeutet der Einsatz durch die damit verbundene Erhebung biometrischer Daten einen im Vergleich zu herkömmlichen Verfahren stärkeren Eingriff in die Persönlichkeitsrechte der Arbeitnehmer, daher die o.a. erforderliche Abwägung.

7

Grundsätzlich ist die Verwendung personenbezogener Daten zur Erfüllung eigener Geschäftszwecke zulässig gemäß § 28 As. 1 Satz 1 Nr. 1 BDSG, sofern sie der "Zweckbestimmung eines Vertragsverhältnisses (...) mit dem Betroffenen dient." Da der Zweck eines Arbeitsverhältnisses vor allem in der leistungsgerechten Erbringung der Arbeitskraft durch den Beschäftigten gegen eine adäquate Entlohnung liegt, darf der Arbeitgeber jedenfalls bestimmte Daten über die Person des Beschäftigten verwenden und zur Kontrolle der Arbeitsleistung die Verwendung der betrieblichen Arbeitsmittel in gewissen Grenzen kontrollieren.

8

Zu beachten ist hierbei, dass dieses Muster vor allem auf die Nutzung eines biometrischen Systems im Betrieb allgemein ausgerichtet ist und Aspekte, die etwa grundsätzlich ein Zutrittskontrollsystem betreffen, hier nicht im Einzelnen berücksichtigt sind und ggfs. noch ergänzt werden müssen. Dies gilt auch für grundsätzliche Pflichten des Arbeitgebers, die hier nur Biometrie spezifisch aufgenommen wurden und daher nicht vollständig abgebildet sind.

9

Hier sollten allgemeinverbindliche Prinzipien und Grundsätze genannt werden, die bei evtl. später auftretenden Auslegungsschwierigkeiten oder Streitigkeiten herangezogen werden können und auch Anhaltspunkte dafür liefern, welche Intention die Parteien beim Abschluss der Betriebsvereinbarung verfolgten.

10

Es wird der Begriff der Beschäftigten genutzt, um einen einfach geschlechtsneutral zu formulierenden Begriff für die Arbeitnehmerinnen und die Arbeitnehmer des Unternehmens zu nutzen. Eine andere Definition des Arbeitnehmerbegriffs ist damit nicht verbunden.

11

Erforderlich ist hier eine Abwägung der verschiedenen Interessen. Das Sicherheitsbedürfnis des Arbeitgebers, das zur Einführung des biometrischen Systems führt, muss im Verhältnis zu den durch diesen Einsatz berührten Persönlichkeitsrechten der Arbeitnehmer angemessen abgewogen werden. Der Einsatz des biometrischen Systems muss also in diesem Rahmen verhältnismäßig sein, d.h. notwendig zur Sicherung betrieblicher Interessen sein bei gleichzeitiger Wahrung der Persönlichkeitsrechte der Arbeitnehmer.

Zu berücksichtigende Zulässigkeits- und Gestaltungskriterien sind u.a. (diese finden sich unter verschiedenen Aspekten in den Einzelheiten der hier vorgeschlagenen Betriebsvereinbarung wieder):

- Technische Leistungsfähigkeit des Systems (Berücksichtigung der Erkennungsleistung sowie der Sicherheit),
- Erforderlichkeit des Einsatzes,
- Zweckbestimmung und -bindung,
- Transparenz,
- Technische Gestaltung,
- Gewährleistung der Datensicherheit nach § 9 BDSG und Anlage.

12

Die klare und möglichst umfassende Definition des Gegenstands der Betriebsvereinbarung muss erfolgen. Hier sollte unmissverständlich bestimmt werden, welcher Sachverhalt durch die Betriebsvereinbarung geregelt wird.

13

Sollte der betreffende Betrieb über mehrere Standorte verfügen, und das biometrische System nur an einem dieser Standorte zum Einsatz kommen, ist dies hier anzupassen. Entsprechendes gilt, wenn unterschiedliche Systeme in unterschiedlichen betrieblichen Standorten mit unterschiedlichen Einsatzzwecken eingesetzt werden sollen.

14

Zwar hat der Arbeitgeber auf die dortigen Verhältnisse keinen unmittelbaren Einfluss. Er gibt aber den entsandten Arbeitnehmern die mitbestimmungspflichtigen Anweisungen. Daher ist zwischen ihm und dem Betriebsrat zu vereinbaren, ob und in welcher Weise die Arbeitnehmer der Kontrolle durch biometrische Systeme in einem fremden Betrieb unterworfen werden. Der Arbeitgeber muss bei der Vertragsgestaltung mit dem Kunden dafür sorgen, dass die mit dem Betriebsrat getroffenen Vereinbarungen umgesetzt werden. Individualrechtliche Rechtspositionen der betroffenen Arbeitnehmer bleiben hiervon unberührt. Dies gilt nach jüngster Rechtsprechung des Bundesarbeitsgerichts, vgl. BAG Beschluss vom 27.01.2004, 1 ABR 7/03, AP Nr. 40 zu § 87 BetrVG Überwachung. Dies muss noch weiter ausgeführt werden, wenn der Fall zutrifft.

15

Eine solche zeitliche Beschränkung ist u.U. sinnvoll, wenn der Einsatz von vornherein auf einen bestimmen Zeitraum beschränkt werden soll.

16

Hier ist das konkrete Bedürfnis des Arbeitgebers zu formulieren und der Einsatz des biometrischen Systems zu begründen. Im Folgenden wird beispielhaft von einem Sicherheitsbedürfnis ausgegangen. Der Einsatz eines biometrischen Systems kommt auch aus anderen, gerechtfertigten Gründen in Betracht.

17

XY, hier benennen; alternativ: Zugangs-/Zugriffsverfahren, etc.

18

Hier sind die Gründe aufzuzählen, etwa: Arbeitnehmer ihre Karten getauscht haben, das System anderweitig umgangen wurde, es nicht verfügbar oder funktionsbereit war, Karten und/oder Passwörter/Geheimzahlen abhanden gekommen sind, Arbeitnehmer ihre Karten vergessen haben, etc.

19

Hier soll die gewählte Betriebsart dargestellt werden, sowie die Abwägung der Interessen, Gründe (zu erreichender Zweck), Erforderlichkeit der Datenverwendung, unter Verweis auf nicht sinnvolle/zumutbare Alternativen, z.B. Verweise auf Sicherheit, etc.

20

Hier sollten wenn möglich konkrete Zahlen benannt werden, also: welches System, wie wurde die Pilotierung durchgeführt etc.

21

Diese Informationen sollte Idealerweise sich an den notwendigen Inhalten der "informierten" Einwilligung nach BDSG orientiert werden.

22

Diese Informationen müssen eine Vorstellung des zum Einsatz kommenden biometrischen Systems enthalten, anhand derer sich die betroffenen Arbeitnehmer darüber informieren können, was ein biometrisches System ist, wie der Erkennungsvorgang selbst funktioniert und warum der Einsatz eines solchen als notwendig erscheint (s. auch oben betr. "Informationsveranstaltung").

23

Aus Vereinfachungs- und Kostengründen wird hier zum Erhalt des alten Zutrittskontrollsystems geraten. Daneben kommt eine manuelle Kontrolle etwa durch einen Pförtner (falls vorhanden) in Betracht.

24

Diese Entscheidung muss allerdings bereits im Vorfeld, also am besten während der Pilotierungsphase, getroffen werden, und wird hier nur der Vollständigkeit halber aufgeführt. In der Betriebsvereinbarung ist hier das gewählte Ersatzsystem zu benennen.

25

Weitere Ausführungen hierzu finden sich im TeleTrusT Kriterienkatalog, s. dort 3.2.7 und 8.5.

26

Die vor den Verhandlungen zu dieser Betriebsvereinbarung durchgeführte Pilotierungsphase sollte möglichst erwiesen haben, dass bei einem Einsatz des geplanten biometrischen Systems das Sicherheitsbedürfnis des Arbeitgebers in erhöhtem Maße erfüllt wird. Allerdings ist im Gegenzug das Persönlichkeitsrecht der Arbeitnehmer einem erhöhten Risiko ausgesetzt. Diese potenzielle Gefährdung steht nur dann dem betrieblichen Einsatz nicht entgegen, wenn das berechtigte Interesse wie etwa das Sicherheitsbedürfnis überwiegt und der Arbeitgeber nachweisen kann, dass das konkrete System sicher gegenüber Überwindungsversuchen und gegen Missbrauch ist. Die Sicherheit des einzusetzenden biometrischen Systems ist in jedem Fall auf die betrieblichen Belange anzupassen. Hohe Sicherheit geht in der Regel einher mit eingeschränktem Komfort für den Benutzer, da die für die Sicherheit verantwortliche Falschakzeptanzrate (also die Rate, die darüber Auskunft gibt, wie viele Unberechtigte vom System fälschlich als berechtigt zugelassen werden) eng mit der Falschzurückweisungsrate (also die Rate, die darüber Auskunft gibt, wie viele Berechtigte vom System fälschlicherweise als unberechtigt abgewiesen werden) korreliert ist. Eine FAR von 0 % und damit hundertprozentige Sicherheit kann in keinem Fall erreicht werden.

27

Die Erforderlichkeit einer Lebenderkennung ist anwendungsbezogen zu bestimmen und auch nicht bei allem erhältlichen biometrischen Systemen gegeben.

28

Bei der Pilotierung sollte bereits über die Hinzuziehung eines professionellen und Biometrieerfahrenen, möglichst herstellerneutralen Anbieters nachgedacht werden.

29

Dass das BDSG bzw. das entsprechenden Landesdatenschutzgesetz gilt, muss nicht erwähnt werden, da dies ohnehin je nach Anwendungsgebiet der Fall ist.

30
Bzw. bezogen auf eine andere konkret beabsichtigte Nutzung.

31
Beim Einsatz biometrischer Systeme innerhalb eines Betriebs ist der Datenschutz von größter Bedeutung. Deshalb muss eine derartige Zweckbindung eingehalten werden, dass die biometrischen Daten nur für eben den Einsatz erhoben, verarbeitet und genutzt werden, für den sie bereits vorher festgelegt wurden. Hier kommt es darauf an, dass der Zweck des Einsatzes vor der Einführung des biometrischen Systems festgelegt und hier in der Betriebsvereinbarung genau definiert wird. Dabei ist auch die Speicherungsdauer genau festzuschreiben und konsequent einzuhalten. Eine Auswertung über die reine Überprüfung der Berechtigung gemäß der vorab festgelegten Zweckbestimmung hinaus ist unzulässig. Dafür sind geeignete technische und organisatorische Maßnahmen zu treffen.

32
z.B. für Zwecke der Strafverfolgung möglich

33
Aus datenschutzrechtlicher Sicht ist grundsätzlich eine zentrale Datenerhebung und -speicherung zu vermeiden und eine dezentrale Speicherung vorzuziehen. Sollte jedoch eine zentrale Datenhaltung erforderlich sein, ist der Betrieb im Verifikationsmodus dem Betrieb im Identifikationsmodus vorzuziehen. Eine zentrale Datenhaltung bedeutet im Betrieb konkret, dass die biometrischen Daten der Beschäftigten nicht auf einer Chipkarte oder einem anderen Token gespeichert sondern auf einem zentralen Server abgelegt werden. Nur wenn geeignete Schutzmaßnahmen getroffen werden können, ist eine solche Verfahrensweise als datenschutzrechtlich zulässig anzusehen (siehe auch nachfolgende Erläuterung).

In der Betriebsvereinbarung muss grundsätzlich - auch im Interesse der Datensparsamkeit - präzise festgelegt werden, ob Verifikation oder Identifikation erfolgt, ob Rohdaten oder Templates gearbeitet wird, ob die Protokollierung auf der Karte, am Lesegerät dezentral oder auf einem zentraler Server erfolgt, ob die biometrischen Daten nur auf der Karte gespeichert werden oder (auch) im Hintergrundsystem (zwecks Verifikation/Identifikation oder nur als Back-Up), abgespeichert werden (vgl. Fn. 16). Die Zwecke sollten präzise benannt werden, z.B. Datensicherheit bei IT-Räumen, Verhinderung von Diebstählen, sichere IT-Nutzung (s. dazu auch das BSI-Grundschutzhandbuch, www.bsi.bund.de).

34
Vgl. Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1. Juni 2005: „Einführung biometrischer Ausweisdokumente“, http://www.bfd.bund.de/information/DS-Konferenzen/69_70_ent1.html

35
Hier sollte für jede Anwendung gesondert eine Risikoanalyse stattfinden. Dabei sind die möglichen Alternativen zu evaluieren und ein Bericht zu erstellen, der mindestens Arbeitgeber, Betriebsrat und betrieblichem Datenschutzbeauftragten verfügbar gemacht werden sollte. Sollte für die konkrete Anwendung dennoch eine zentrale Datenhaltung und der Betrieb des Systems im Identifikationsmodus erforderlich sein, muss dies entsprechend begründet werden und die getroffenen Sicherheitsmaßnahmen auch gegen Missbrauch der biometrischen Daten und weiteren Angriffen aufgeführt werden. Der Identifikationsmodus kann möglicherweise dann erforderlich sein, wenn die Beschäftigten wegen der Besonderheit der betrieblichen Umgebung keine Token bei sich führen können oder sollen. Hier sollten alle in Betracht kommenden Alternativen wie z.B. auch die Nutzung kontaktloser Token zu berücksichtigt werden.

36

Eine Speicherung von Daten bei Matchingvorgängen über den Zeitraum hinaus, der zum Matching erforderlich ist, ist zu vermeiden. Soweit möglich sollten Verfahren der Anonymisierung und Pseudonymisierung verwendet werden.

37

Das eingesetzte Verschlüsselungsverfahren und die anderen Sicherungsverfahren sind zu benennen und ihre Geeignetheit zum Schutz der biometrischen Daten nachzuweisen.

38

Eine solche beinhaltet die Prüfung vor Beginn der Verarbeitung der personenbezogenen Daten. Während diese nach Bundesdatenschutzrecht nur bei besonderen Risiken für die Rechte und Freiheiten der Betroffenen durch automatisierte Verarbeitungen angezeigt ist, enthält etwa das hessische Landesdatenschutzrecht eine derartige Einschränkung nicht.

39

Ein solches Datenschutzaudit ist optional und kann zur Verbesserung des Datenschutzes und der Datensicherheit die Prüfung und Bewertung des Datenschutzkonzepts sowie der technischen Einrichtungen des Unternehmens durch unabhängige und zugelassene Gutachter beinhalten. Durch Veröffentlichung des Ergebnisses der Prüfung kann sich das Unternehmen im Wettbewerb positiv hervorheben.

40

Bei Erhebung, Verarbeitung und Nutzung der biometrischen Daten ist in datenschutzrechtlicher Hinsicht zur Wahrung der Persönlichkeitsrechte der Arbeitnehmer auf die im Folgenden aufgeführten Aspekte nach BDSG besonders zu achten. Mit diesen Maßnahmen sind die datenschutzrechtlichen Anforderungen konkret umzusetzen. Die im Folgenden aufgeführten Kriterien sind sowohl bei einer zentralen als auch bei einer dezentralen Speicherung der biometrischen Daten zu beachten, wobei stets die Besonderheit der konkret gewählten Betriebsart des biometrischen Systems zu berücksichtigen sind. Die betrieblichen IT-Beauftragten/die entsprechende Abteilung ist zur Umsetzung mit einzubeziehen. Im IT-Sicherheitskonzept des Betriebs ist der Umgang mit den biometrischen Daten der Arbeitnehmer gesondert zu berücksichtigen.

41

Hier ist zu beachten, dass auch die Wartung des Systems Auftrags-Datenverarbeitung im Sinne von § 11 Abs. 5 BDSG ist.

42

Eine regelmäßige Überprüfung wird empfohlen, um zu überprüfen, ob das System noch den Sicherheitsbedürfnissen des Arbeitgebers unter gleichzeitiger Wahrung der Persönlichkeitsrechte der Arbeitnehmer entspricht. Es handelt sich hierbei nicht um eine ausdrückliche gesetzliche Verpflichtung.

43

Hier sollte festgelegt werden, wann dies der Fall ist. Beispiele: Eine solche liegt dann vor, wenn bei einer FAR von 1 % die FRR auf über 10 % über einen Zeitraum von drei Monaten angestiegen ist bzw. die Nutzungsdauer für jeden Erkennungsvorgang über einen protokollierten Zeitraum von über drei Monaten auf über 5 Minuten steigt oder missbräuchliche Umgehungen des Systems erfolgt sind.

44

§ 77 Abs. 4 BetrVG schreibt vor, dass eine BV eingehalten werden muss. Streitigkeiten über die Durchführung von Betriebsvereinbarungen berechtigen den Betriebsrat zur Einleitung eines Beschlussverfahrens beim Arbeitsgericht (BAG v. 24.2.1987, AP Nr. 21 und 24 zu § 77 BetrVG 1972).

Stellt der Betriebsrat fest, dass der Arbeitgeber z.B. gegen das BDSG verstößt, kann er dies gegenüber dem Arbeitgeber beanstanden und ggf. den betrieblichen Datenschutzbeauftragten und die zuständige Aufsichtsbehörde für den Datenschutz hinzuziehen.

45

Nach § 77 Abs. 5 BetrVG besteht eine dreimonatige Kündigungsfrist. Allerdings können auch abweichende Fristen vereinbart werden. Bei einer Betriebsvereinbarung, die von vornherein auf eine begrenzte Gültigkeitsdauer abzielt, indem eine feste Laufzeit vereinbart wird, ist eine gesonderte Kündigung nicht notwendig. Der ersatzlose Wegfall der Betriebsvereinbarung wird aber nur erreicht, wenn keine Nachwirkung vereinbart wurde.

46

Wenn in der Folge nicht eine wirksame Einwilligung eines jeden Arbeitnehmers eingeholt wird, kann dieser die Nutzung des biometrischen Systems dann ohne arbeitsvertragliche Auswirkungen verweigern.

S C H L U S S