Biometrie im betrieblichen Einsatz

Einleitung

Die Regelungen der UVV-Kassen C9, insbesondere der BGI 819 1,2,3 schreiben im Geschäftsstellenkonzept der PLUS-Lösung und Kleinstzweigstellen den Einsatz biometrischer Systeme vor. Zeitverschlussbehältnisse und Hintergrundbestände sind mit in das biometrische System zu integrieren.

Nach den Regelungen des Betriebsverfassungsgesetzes unterliegt die betriebliche Einführung eines biometrischen Systems der Mitbestimmung des Betriebsrats. Dieses Mitbestimmungsrecht umzusetzen ist Sinn und Zweck einer Betriebsvereinbarung. Diese Orientierungshilfe soll als Vorschlag dienen und dazu beitragen, die wesentlichen Aspekte bei der Erstellung einer Vereinbarung zu beachten.

Auch für solche Unternehmen, Banken und Sparkassen, 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.

Dieses Dokument ist entstanden durch Erfahrungen bei der Einführung biometrischer Systeme und das Zusammentragen aktuell gültiger Datenschutzbestimmungen und Rechtsprechungen, sowie auf Grundlage von Informationen aus Seminaren und Fachkonferenzen (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., Bundesamt für Sicherheit in der Informationstechnik, Datenschutzbeauftragte, etc.).

Betriebsvereinbarung (Orientierungshilfe, Muster)

Zwischen dem Vorstand der *Bank/Sparkasse* _____ und dem Betriebsrat der *Bank/Sparkasse* _____ über den betrieblichen Einsatz biometrischer Systeme im Rahmen von Zutritts- oder Zugangs- / Zugriffssicherung (bzw. andere Sicherheitsanwendungen im Rahmen der UVV-Kassen).

1. Präambel

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 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.

2. Allgemeines

2.1. Gegenstand

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 SAFECOR GmbH genutzt werden, unabhängig vom Standort dieser Systeme.

2.1.1 Geltungsbereich

Die Betriebsvereinbarung gilt für alle Beschäftigten der *Bank/Sparkasse* und in Bezug auf sämtliche im Arbeitsbereich der Beschäftigten zum Einsatz kommenden biometrischen Systeme, wobei es keine Rolle spielt, wo sich diese Systeme befinden.

2.2. Geltungsdauer

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

3. Inhaltliche Regelungen

3.1. Ziele und Gründe des Einsatzes biometrischer Verfahren

Der Betrieb der Geschäftsstellen nach den Regelungen der Unfallkassen schreibt den Einsatz biometrischer Systeme in PLUS-Stellen vor. Ziel jener Sicherungsmaßnahmen ist die Prävention und die Reduzierung der Gefährdungen durch Überfälle. Aus diesem Grund ist es wegen des berechtigten Sicherheitsbedürfnisses des Arbeitgebers notwendig, biometrische Sicherungskonzepte einzusetzen. Das geplante biometrische System verspricht die Befriedigung dieses Bedürfnisses unter gleichzeitiger Wahrung der Persönlichkeitsrechte der Arbeitnehmer. Ziel des Einsatzes des biometrischen Systems ist es, die Geschäftsstellen sicherer zu gestalten.

3.2. Transparenz

Um die Akzeptanz des biometrischen Systems in der Praxis zu erhöhen, ist eine Transparenz über das biometrische System, seine Notwendigkeit und die Verarbeitung der biometrischen Daten zu gewährleisten. Zu diesem Zweck kann es zielführend sein, eine Information der Arbeitnehmer über die genannten Aspekte vor oder während des laufenden Betriebs auszugeben. Ferner kann ein

Ansprechpartner benannt werden, mit dessen Hilfe sich die Beschäftigten bei Problemen oder Fragen informieren können. Schließlich sind Mitglieder der Arbeitnehmervertretung sowie der betriebliche Datenschutzbeauftragte bzw. weitere Verantwortliche im notwendigen Umfang zu informieren oder zu qualifizieren.

3.3. Sicherheitsaspekte

Ein besonderes Augenmerk gilt der Erkennungsleistung und Sicherheit des biometrischen Systems. Es gilt die Sicherheit, als auch den Nutzerkomfort für beiden Parteien als akzeptabel abzuwägen. Das einzusetzende biometrische System verfügt darüber hinaus über Möglichkeiten der Falscherkennung.

3.4. Datenschutz

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

3.4.1. Zweckbindung

Die biometrischen Daten der Arbeitnehmer werden nur für Zwecke der genannten Sicherheits-Systeme erhoben, verarbeitet und genutzt. Eine Weitergabe in nicht anonymisierter Form an Dritte oder auch andere Unternehmensbereiche ist unzulässig. Es findet keine Leistungs- oder Verhaltenskontrolle unter Verwendung der biometrischen Daten statt.
Bei einer gesetzlich erlaubten Zweckänderung 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.

3.4.2. Datenschutz - Datenerhebung und -speicherung

Das biometrische System kann im Identifikations- oder Verifikationsmodus betrieben werden. Bei dem biometrischen Identifikationssystem der Firma SAFECOR (kurz: OSsecure) 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 Minutien, welche die relevanten Punkte des Fingerabdrucks charakterisieren. Diese Merkmale sind besonders die Verzweigungsstellen der Furchen und Stege der Hautoberfläche.

Das biometrische System ist mehrfach gegen Manipulation oder Datenmissbrauch gesichert. Die wesentlichen und entscheidenden Sicherungsmerkmale bestehen zum einen in der "Minimierung" der aufgenommenen Fingerabdrücke und weiterhin in der verschlüsselten Speicherung dieser. Es erfolgt somit keine Speicherung des Fingerabdruck-Bildes, sondern es werden nur die extrahierten biometrischen Referenzmerkmale in digitaler Form gespeichert (Template). Das Bild des Fingerabdrucks wird vom OSsecure System verarbeitet und es werden die eindeutigen Erkennungsmerkmale des Fingerabdrucks für den späteren Vergleich verschlüsselt abgelegt, was einen Missbrauch, z.B. durch Reproduktion des Fingerabdrucks, unmöglich macht. Der Fachbegriff für dieses Verfahren nennt sich "Biometric Template Protection".
Entscheidend ist bei dem OSsecure-Verfahren, dass nicht die Bilder oder Templates selbst hinterlegt werden, sondern binäre Daten, die alleine keine Rekonstruktion der biometrischen Bilder ermöglichen. Darüber hinaus greift ein zusätzlicher (gängiger) "Kryptoschutz".

3.4.3. Datenschutz - Datenvermeidung und Datensparsamkeit

Es werden lediglich die Daten erhoben und gespeichert, die für die eigentliche Erkennung

auch tatsächlich notwendig sind. Die erfassten Daten werden weiterhin auf ein Minimum reduziert und verschlüsselt. Falls trotzdem ein Informationsüberschuss entsteht, wird eine weitergehende Verwendung ausgeschlossen.
Sowohl Datenvermeidung und -sparsamkeit als auch 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. Der Arbeitgeber verpflichtet sich, ein Datenschutzaudit nach § 9a BDSG durchzuführen.

3.4.4. Datenschutz - Löschungsfristen

Nach Ausscheiden eines Arbeitnehmers aus der *Bank/Sparkasse* sind die entsprechenden biometrischen Daten vollständig und unwiederbringlich aus dem OSsecure-System zu löschen.

3.5. Technische und organisatorische Maßnahmen

Der Arbeitgeber hat die wirksame Umsetzung der nach § 9 und Anlage zu § 9 BDSG bzw. dem entsprechenden Landesdatenschutzgesetz erforderlichen technischen und organisatorischen Maßnahmen sicherzustellen. 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.

3.5.1. Zutrittskontrolle

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

3.5.2. Zugangskontrolle

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

3.5.3. 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.

3.5.4. Weitergabekontrolle

Zu gewährleisten hat der Arbeitgeber weiterhin, dass biometrische Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung von Unbefugten nicht gelesen, verändert oder entfernt werden können. Zudem ist durch geeignete Maßnahmen wie z.B. eine revisionssichere Protokollierung zu gewährleisten, dass überprüft und festgestellt werden kann, wann und durch wen biometrische Daten erfasst wurden.

3.5.5. Auftragskontrolle

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

3.6. 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 die Einführung des Systems zuzuleiten.

4. Schlussvorschriften

4.1. Verfahren bei Streitigkeiten

Bei allen Streitigkeiten, die aus dieser Betriebsvereinbarung entstehen, kann die *Bank/Sparkasse* oder der Betriebsrat die Einigungsstelle gem. § 76 BetrVG anrufen. Die Parteien unterwerfen sich bereits jetzt dem Spruch der Einigungsstelle.
Verstöße gegen die Betriebsvereinbarung
Verstöße gegen die in dieser Betriebsvereinbarung aufgestellten Regelungen sind entsprechend zu sanktionieren.

4.2. 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.

4.3. Inkrafttreten, Kündigung

Diese Vereinbarung tritt am _____ in Kraft und kann mit einer Frist von drei Monaten zum Jahresschluss, erstmals zum _____ gekündigt werden. Ist diese Betriebsvereinbarung wirksam gekündigt, so wirkt diese bis zum Abschluss neuer Vereinbarungen nach und verliert nicht ihre Bedeutung als Rechtsgrundlage im Sinne von § 4 Absatz 1 BDSG46. Die Parteien vereinbaren ausdrücklich eine Nachwirkung i. S. d. § 77 Abs. 6 BetrVG.