Betriebsvereinbarung zum Thema Zutrittskontrolle - Gebäude und Bereiche

Zwischen der Firma […]

und

dem Betriebsrat der Firma […]

wird folgende Betriebsvereinbarung geschlossen:

§ 1 Geltungsbereich und Zweckbestimmung

1. Die Betriebsvereinbarung gilt für alle Beschäftigten der […] in […].
2. Die Betriebsvereinbarung regelt die Einrichtungen der […] in verschiedene Zutritts- und sicherheitsrelevante Bereiche, den Zutritt der Mitarbeiter in zu diesen Bereichen sowie die Verwendung der hierfür bestimmten technischen Systeme und deren Auswertungen.
3. Eine Leistungskontrolle findet nicht statt. Personenbezogene der personenbeziehbare Daten, die für eine Verhaltenskontrolle geeignet sind, dürfen, mit Ausnahme von § 4, nicht dafür verwandt werden.

§ 2 Zutritts- und sicherheitsrelevante Bereiche

Die Einrichtungen der […] werden in die aus der §1 ersichtlichen Zutritts- und sicherheitsrelevanten Bereiche aufgeteilt. Es wird durch die […] sichergestellt, dass jeder Mitarbeiter die Zutrittsberechtigungen erhält, die er zur Erfüllung seiner Aufgaben benötigt. Jedem Mitarbeiter wird für den Zutritt zu bestimmten Zutritts- und sicherheitsrelevanten Bereichen eine Berechtigung zugeteilt. Je nach Tätigkeit ist auch die Zuteilung mehrerer Berechtigungen möglich. Der Zutritt zu den verschiedenen Zutritts- und sicherheitsrelevanten Bereichen ist nur durch einen entsprechenden Ausweis oder PIN-Code möglich. Ausnahmen davon sind in § 5 bzw. § 6 geregelt.

§ 3 Zutrittskontrollsystem

Die Zutrittskontrolle wird durch das Zutrittskontrollsystem geregelt. Dieses System besteht aus einem oder mehreren Zutrittsterminal pro Zutritt- bzw. sicherheitsrelevanten Bereich, welches/welche nach Einlesen der Informationen über die Ausweiskarte / den PIN-Code eines jeden Karteninhabers den Zutritt freigibt und die entsprechenden Daten an den Rechner weiter meldet. Die für die Verarbeitung der auf der Ausweiskarte enthaltenen Informationen notwendigen Kenntnisse der abzugleichenden Daten werden dem Zutrittskontrollsystem über das Personalwirtschaftssystem mitgeteilt. Hierbei findet lediglich ein täglicher Datenfluss statt. Folgende Daten werden von SAP R/3 HR zum INCA-Rechner übermittelt:

- Personalnummer
- Ausweisnummer
- Name, Vorname
- PIN-Nummer
- Über einen in der Sourcing und Logistics Section der […] installierten Bildschirmarbeitsplätze besteht eine passwortgeschützte Zugriffsmöglichkeit auf die im Rechner vorgehaltenen Daten. Eine detaillierte Beschreibung der Hard- und Software-Bestandteile des Zutrittskontrollsystems ergibt sich aus Anlage …

Das Zutrittskontrollsystem erfüllt danach folgende Funktionen

Freigabe/Nichtfreigabe des Zutritts
Speicherung der Zutrittsdaten (Datum, Zeit, Ausweis-Nr., PIN-Code, Name, Terminal)Demnach wird grundsätzlich zwischen 3 Datenarten unterschieden:

a. Systemdaten: Betriebssystem, Programmdateien und Protokolldateien gemäß der besonderen Zweckbindung des § 31 BDSG.
b. Zutrittsberechtigungsdaten: Ausweisnummer der Zugangskarte, PIN-Code der Zugangskarte, räumliche und zeitliche Zuordnung der Zutrittsberechtigung, Zuordnung der Ausweisnummer der Zugangskarte zum Benutzer, Angaben zum Karteninhaber.
c. Ereignisdaten: Kartennummer der Zugangskarte, PIN-Code der Zugangskarte, Datum und Uhrzeit des Zutritts, Anzahl der Zutrittsversuche. (Eine Erfassung der Daten bei Verlassen der Räume findet nicht statt).

Die verwendeten Zugangskarten sind nach heutigem Stand der Technik so fälschungssicher wie möglich gestaltet. Die Kartenleser sind so beschaffen, dass Lesevorgänge ausschließlich durch den Benutzer in Gang gesetzt werden können. Dieser Lesevorgang muss für den Benutzer nachvollziehbar sein. Automatische Lese- oder sonstige Erkennungsvorgänge, die eine nicht bemerkbare Überwachung ermöglichen, sind ausgeschlossen. Daten aus dem Zutrittskontrollsystem dürfen in keiner Form an andere Systeme übergeben werden.

§ 4 Auswertungen

Auswertungen sind zulässig, wenn konkrete Anhaltspunkte für das Vorliegen einer Straftat vorhanden sind, an der Mitarbeiter oder Externe beteiligt waren. Auswertungen im Sinne dieser Vereinbarung sind nur aus aktuellem Anlass erlaubt. Der Betriebsrat ist vor jeder Auswertung zu informieren. Er hat ein Einspruchsrecht. Im Fall des Einspruchs darf die Auswertung nicht vorgenommen werden. Von der XXXXX werden ein Systemadministrator und ein Vertreter benannt. Der Systemadministrator ist zuständig für den laufenden Betrieb des Systems. Die Aufgaben des Systemadministrators und der Sourcing und Logistics Section der XXXXX sind personell strikt voneinander zu trennen. Die Person(en), die mit der Administration der Zutrittsberechtigungsdaten betraut ist/sind, ist/sind dem Betriebsrat namentlich zu benennen. Ihre Aufgabe ist die Verwaltung der Zutrittsberechtigungsdaten. Sie haben keine Zugriffsrechte auf die Ereignisdaten. Solche Zugriffe sind nur im 4-Augen-Prinzip, zusammen mit einem Beauftragten des Betriebsrates erlaubt. Das 4-Augenprinzip beinhaltet ein Passwort, das ausschließlich dem Betriebsrat bekannt ist.

Der Betriebsrat erhält auf Wunsch von jeder entsprechenden Auswertung eine Durchschrift. Die durch das System möglichen Auswertungen sind in Anlage 3 beschrieben und abschließend. Es besteht weiter Einvernehmen zwischen den Parteien, dass die Speicherdauer der über die Zutrittsterminals per up load in den INCA-Rechner geladenen Daten (Ereignisdaten) einen Zeitraum von sechs Monaten nicht überschreiten darf. Ereignisdaten, die älter als sechs Monaten sind, werden gelöscht.

§ 5 Zutrittsberechtigung für Mitarbeiter der […]

Jeder Mitarbeiter der […] erhält einen Kartenausweis und gegebenenfalls eine PIN-Code Nummer, welche ihm entsprechend seiner Berechtigung den Zugang zu den Zutritts- bzw. zu den sicherheitsrelevanten Bereichen eröffnen. Der Ausweis ist bei Zutritt zu den Zutritts- und den sicherheitsrelevanten Bereichen an den dort installierten Zutrittsterminals zu verwenden; die PIN-Code-Nummer ist an den

vorgesehenen Geräten einzugeben. Auf Verlangen des Sicherheitsdienstes ist der Kartenausweis dem entsprechenden Sicherheitspersonal zur Kontrolle vorzulegen.

Die Mitnahmen unbekannter Personen, ohne dass diese eine besondere Zugangsberechtigung als Besucher erhalten haben, ist verboten. Der Ausweis ist so aufzubewahren, dass er möglichst vor Verlust gesichert ist; die Mitarbeiter werden dabei darum gebeten, die Sorgfalt aufzuwenden, die sie bei Aufbewahrung von Kreditkarten an den Tag legen.

Die PIN-Code Nummer ist geheim zu halten. Der Verlust der Ausweiskarte ist nach Bemerken des Verlustes unverzüglich der Sourcing und Logistics Section der […] zu melden. Hat ein Mitarbeiter seinen persönlichen Ausweis vergessen, so kann er für den jeweiligen Arbeitstag ersatzweise eine Zutrittskarte vom Sicherheitsdienst erhalten. Auf Verlangen hat er sich gegenüber dem Sicherheitsdienst entsprechend aus zuweisen. Sollte ein Mitarbeiter der XXXXX in einen sicherheitsrelevanten Bereich gelangen wollen, für welchen er keinerlei Zutrittsberechtigung hat, so hat er sich bei dem entsprechenden Fachbereich anzumelden. Sofern die Notwendigkeit des Zutritts von einem Mitarbeiter des entsprechenden Bereiches bestätigt wird, wird er persönlich am Zutrittsterminal abgeholt und bei Verlassen wieder zurück begleitet.

§ 6 Zutrittsberechtigung für Dritte

Auf Antrag einer Fachabteilung, für welche Externe aufgrund eines Werk- oder Dienstvertrages länger als eine Woche in einem Zutritts- oder sicherheitsrelevanten Bereich tätig werden sollen bzw. als Drittunternehmer tätig werden (sog. "Permanent Externe"), kann die Sourcing und Logistics Section der […] eine zeitlich auf maximal drei Monate befristeter Zutrittsberechtigung für bestimmte Zutritts- und sicherheitsrelevante Bereiche erteilen. Nach Ablauf der drei Monate erlischt automatisch systemseitig die Berechtigung. Eine Verlängerung der Zutrittsberechtigung ist möglich. Dem Betriebsrat wird auf Anfrage eine Liste der für diesen Personenkreis ausgestellten Zugangskarten zur Verfügung gestellt, aus der sich das Ausgabedatum der Zugangskarte, die Person, das Drittunternehmen, die Zugangsberechtigung und der Zugangsbereich ergibt. Sonstige Dritte, welche Zutritt zu einem sicherheitsrelevanten Bereich begehren, dürfen lediglich nach Anmeldung beim Sicherheitsdienst und entsprechender Bestätigung des Abteilungsleiters (oder der vom Abteilungsleiter benannten Person(en)) des sicherheitsrelevanten Bereiches, in welchen sie gelangen möchten, Zutritt erhalten. Sie müssen daher vom Zutrittsterminal abgeholt und bei Verlassen des Bereiches wieder dorthin zurückbegleitet werden. Es ist sicherzustellen, dass diese Besucher sich nicht ohne Begleitung von Mitarbeitern der XXXXX AG in sicherheitsrelevanten Bereichen aufhalten.

§ 7 Beendigung des Arbeitsverhältnisses

Bei Beendigung des Arbeitsverhältnisses ist die Ausweiskarte vom Mitarbeiter unaufgefordert zurückzugeben.

§ 8 Rechte und Pflichten der Beschäftigten, die am Zutrittskontrollsystem teilnehmen

1. Alle Arbeitnehmer werden umfassend und in geeigneter Weise über die Wirkungsweise des gesamten Systems informiert.
2. Weiterhin erhalten die Beschäftigten, die am Zutrittskontrollsystem teilnehmen, eine schriftliche Mitteilung über alle, ihre Person betreffenden, gespeicherten Datensätze zu Beginn des Systembetriebs.
3. Personelle Entscheidungen dürfen nicht ausschließlich auf Informationen und Erkenntnissen gestützt werden, die durch den Betrieb des

Zutrittkontrollsystems gewonnen werden. Ausnahmen bilden die in § 4 Satz 1 genannten Fälle.

4. Personelle Maßnahmen, die einen Nachteil für einen Beschäftigten zur Folge haben, weil sie auf Informationen beruhen, die unter Verletzung dieser Vereinbarung gewonnen wurden, oder auf unzulässige oder unrichtige Verarbeitung beruhen, sind unwirksam und werden zurück genommen.

§ 9 Rechte des Betriebsrates

Über Maßnahmen, die das Zutrittskontrollsystem betreffen, ist der Betriebsrat nach seinen Beteiligungsrechten rechtzeitig und umfassend zu unterrichten. Rechtzeitig ist die Unterrichtung dann, wenn sie erfolgt, solange noch unterschiedliche Lösungsalternativen im Interesse der betroffenen Beschäftigten berücksichtigt werden können. Der Betriebsrat hat im Rahmen seiner allgemeinen Aufgaben ein Informations- und Überwachungsrecht bezüglich der Einhaltung der Betriebsvereinbarung (§ 80 BetrVG). Der erforderliche Zutritt zu den entsprechenden Systemen, allen Arbeitsräumen in denen Arbeitnehmer beschäftigt werden und die erforderlichen Informationen sind zu gewähren. Die […] ist verpflichtet, dem Betriebsrat Informationen und Kenntnisse, die sich aus dem Betreiben des Zugangkontrollsystems ergeben, bzw. die zum Betrieb notwendig sind, auf Anfrage zur Verfügung zu stellen.

§ 10 Inkrafttreten und Kündigung

Die Betriebsvereinbarung tritt mit drei Wochen nach Unterzeichnung in Kraft. Sie kann mit einer Frist von drei Monaten zum Monatsende gekündigt werden.