Themen: Biometrie
Berufe: Führungskraft
Datentypen: Biometrie

Darf ich biometrische Daten von meinen Mitarbeitern erheben?

Die Geschäftsleitung möchte es den Mitarbeitern ersparen, für den Zutritt zu den Gebäuden immer einen Magnetschlüssel bei sich führen zu müssen. Daher beschliesst sie, eine biometrische Zutrittskontrolle einzuführen. Die Mitarbeiter werden mittels interner Rundschreiben aufgefordert, ihre biometrischen Daten (Handgeometrie und Fingerabdrücke) zur Verfügung zu stellen.
Drei Angestellte ignorieren die Aufforderung. Als sie sich dazu äussern sollen, erklären sie, ihren Erkundigungen zufolge sei eine solche Massnahme als schwerer Eingriff in die Privatsphäre zu werten, und dass sie sich aus diesem Grund verweigerten.
Die Geschäftsleitung informiert sich genauer darüber, was bei der Einführung eines solchen Systems zu berücksichtigen ist. Sie kontaktiert den Berater für Datenschutzfragen in der Firma oder den Eidgenössischen/Kantonalen Datenschutzbeauftragten. Dann beruft sie eine Mitarbeitervollversammlung ein, um die Vorteile des neuen Systems zu erläutern. Die Mitarbeiter werden darüber informiert, dass die Geschäftsleitung im Kontakt mit der zuständigen Behörde stehe. Ihnen wird zugesichert, dass das System nicht missbraucht werde, dass die Daten sicher aufbewahrt werden etc. Einer der Angestellten lässt sich jedoch nicht abbringen: Es gäbe einfachere Methoden der Zutrittskontrolle wie beispielsweise Magnetkarten. Die Geschäftsführung schlägt daraufhin eine Abstimmung durch Handzeichen vor. Die drei sich widersetzenden Angestellten verlangen eine geheime Abstimmung und setzen diese auch durch.
Nach dem Auszählen der Stimmen wird deutlich: Der Status Quo wurde bestätigt. Die Geschäftsleitung muss eingestehen, dass die vorgesehene Datenerhebung nicht im Verhältnis zum angestrebten Ziel stehe und es daher erforderlich sei, die Einwilligungen jedes einzelnen Angestellten einzuholen. Mit Hinblick auf die Kosten und Komplikationen, die entstünden, wenn beide Verfahren (magnetisch und biometrisch) parallel angewandt würden, stellt sie das Vorhaben zurück und verspricht, nach einer weniger einschneidenden Lösung zu suchen.
Die zur biometrischen Zutrittskontrolle erhobenen Daten könnten zweckentfremdet werden. Die Geschäftsführung ist zufrieden, sich für eine kreative Lösung entschieden zu haben, bei der die Persönlichkeitsrechte der Angestellten berücksichtigt werden.

Empfehlungen
Biometrische Daten beinhalten im Allgemeinen besonders schützenswerte Personendaten (die Gesundheit betreffend). Ist dies der Fall, ist eine Rechtsgrundlage nötig, die Betroffenen müssen über die Verwendung der Daten genauestens aufgeklärt werden und dieser ausdrücklich zustimmen. Das verfolgte Ziel muss klar definiert sein und bei der Wahl der geeigneten Mittel, um dieses zu erreichen, muss der adäquatesten und am wenigsten einschneidenden Massnahme der Vorzug gegeben werden. Diese Massnahme muss auf angemessene Art und Weise kommuniziert werden. Der Arbeitgeber sollte zudem die Arbeitnehmer oder ihre Vertreter zu Rate ziehen und, sofern es keine Rechtsgrundlage gibt, ihre informierte Einwilligung einholen, bevor er automatisierte Systeme zur Verarbeitung von Personendaten einführt.

Grundprinzipien
LIPAD 38 et 42 ; DSG 4 al. 4, 12 und 13 ; ArG 6 ; ArGV3 26 ; OR 328 et 328*b*

Schutz der Persönlichkeit, Arbeitnehmerschutz, Grundsatz der Rechtmässigkeit (Gesetzmässigkeit),

Grundsatz von Treu und Glauben und der Verhältnismässigkeit: Die Massnahme muss angemessen und notwendig und so wenig einschneidend wie möglich sein.

Praxisbeispiel
Die Genfer Privatbank Pictet & Cie benutzt seit 2006 als Zutrittssicherung zu ihren Gebäuden 3D-Verfahren zur Gesichtserkennung. Wie sie es geschafft hat, den 2000 Mitarbeitern ihre Befürchtungen zu nehmen? Durch Kommunikation. Mit dieser Technik kann nicht etwa der Gesundheitszustand einer Person überwacht oder die Privatsphäre verletzt werden. „Manche Mitarbeiter befürchten, dass ein Scan ihres Gesichts schädliche Folgen für ihre Gesundheit hat, was nicht der Fall ist, da die Maschine sie lediglich filmt“, so Jean-Pierre Therre, Sicherheitsbeauftragter der Privatbank. Die Datenbank enthält ausserdem keine Fotos der Angestellten, sondern Analysen ihrer Schädelaufnahmen nach 40.000 Bezugspunkten, die keinerlei Aufschlüsse geben: http://www.1234economy.com/biometrie-et-reconnaissance-faciale-en-3d-comment-la-banque-privee-genevoise-pictet-a-gere-les-resistances