Themen: Biometrie
Berufe: Personalabteilung
Datentypen: Biometrie

Werden bei einer biometrischen Kontrolle für den Zutritt zu Büroräumen die Persönlichkeitsrechte der Angestellten verletzt?

Die Geschäftsleitung hat beschlossen, die magnetische Zutrittskontrolle durch ein biometrisches Verfahren (Netzhauterkennung oder Handgeometrie und Fingerabdrücke) zu ersetzen. Sie gibt diese Umstellung dem Personal bekannt. Der Personalausschuss beruft eine Sitzung ein.
Nach einer regen Diskussion beschliesst der Personalausschuss, die Umsetzung des von der Geschäftsleitung gefassten Plans zu verhindern.
Die Personalabteilung (PA) gerät somit ins Kreuzfeuer. Auf der einen Seite steht die Geschäftsleitung, die von den Vorteilen der Massnahme überzeugt ist und an ihrer Entscheidung nicht rütteln will. Auf der anderen Seite hält der Personalausschuss an seiner Position fest, die Umsetzung einer solchen Massnahme stelle eine Verletzung der Persönlichkeitsrechte der Angestellten dar. Die PA beruft eine gemeinsame Sitzung mit der IT-Abteilung (IT), der Geschäftsleitung und dem Berater (oder Beauftragten) für Datenschutz ein, um mögliche Alternativen abzuwägen.
Nach der Sitzung wird eingeräumt, dass die vorgesehene Datenerhebung nicht im Verhältnis zum Nutzen stehe und es daher erforderlich sei, die Einwilligung aller Angestellten einzuholen. Angesichts der Kosten und Komplikationen, die eine parallele Nutzung beider Methoden (magnetisch und biometrisch) verursachen würde, stellt die Geschäftsleitung ihr Vorhaben zurück und beauftragt die IT-Abteilung, eine weniger einschneidende Lösung zu finden
Die zur biometrischen Kontrolle erhobenen Daten könnten zweckentfremdet werden. Die PA ist zufrieden, eine Lösung gefunden zu haben, bei der die Persönlichkeitsrechte der Angestellten berücksichtigt werden.

Empfehlungen
Biometrische Daten beinhalten im Allgemeinen besonders schützenswerte Personendaten (insbesondere die Gesundheit). In dieser Fall, ist eine Rechtsgrundlage nötig, und 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 passendsten und am wenigsten einschneidenden Massnahme den 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 und 328*b*

Schutz der Persönlichkeit, Arbeitnehmerschutz, Grundsatz der Verhältnismässigkeit (die Massnahme muss 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