Themen: Biometrie
Berufe: Angestellter
Datentypen: Biometrie

Darf man mich dazu auffordern, meine biometrischen Daten zur Verfügung zu stellen?

Ein Angestellter benutzt einen Magnetschlüssel, um zu seinem Arbeitsplatz zu gelangen. Die Geschäftsleitung beschliesst, die magnetische Zutrittskontrolle durch ein biometrisches Verfahren zu ersetzen (Netzhauterkennung oder Handgeometrie und Fingerabdrücke). Sie gibt diese Umstellung dem Personal bekannt.
Der Angestellte erkundigt sich telefonisch bei einer Gewerkschaft, die ihm erklärt, dies sei „absolut illegal“, das Personal solle sich „verweigern“, und eine Entlassung aus diesem Grund wäre „äusserst ungerechtfertigt“. Der Angestellte informiert seinen Vorgesetzten darüber, dass er nicht vorhabe, sich der Erfassung der biometrischen Daten zu unterziehen.
Die Geschäftsleitung erfährt von der Absicht des Angestellten und gibt ihm zu verstehen, dass sie diese mangelnde Kooperation als untragbare Verletzung seines Arbeitsvertrags begreife. Der Vorgesetzte des betroffenen Angestellten wendet sich besorgt an den Datenschutzberater (oder -beauftragten) und organisiert eine Sitzung mit einem Vertreter der Geschäftsleitung, um die Sachlage einzuschätzen.
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. Die Geschäftsleitung stellt ihr Vorhaben zurück und bemüht sich um eine weniger einschneidende Lösung.
Die zur biometrischen Kontrolle erhobenen Daten könnten zweckentfremdet werden. Der Angestellte ist zufrieden, dass er sich mit seinen Befürchtungen Gehör verschafft hat.

Empfehlungen
Biometrische Daten beinhalten im Allgemeinen besonders schützenswerte Personendaten (insbesondere die Gesundheit). Ist dies der 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, 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 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