

# Biometrie und Datenschutz

Die Kontrolle des Zutritts zu Räumen und Gebäuden unter Verwendung biometrischer Merkmale wie dem Fingerabdruck hat gegenüber anderen Systemen wesentliche Vorteile. (Bild: shutterstock)

**Die Wirksamkeit eines Zutrittskontrollsystems hängt wesentlich davon ab, wie sicher berechnigte von unberechnigten Personen unterschieden werden können. Da biometrische Merkmale extrem schwierig zu fälschen sind, gilt die biometrische Identifizierung als sehr sicher. Die erfolgreiche Anwendung dieser Systeme im Privatbereich setzt allerdings voraus, dass den datenschutzrechtlichen Rahmenbedingungen genügend Beachtung geschenkt wird.**



## Maria Winkler

ist mag. iur. und geschäftsführende Partnerin der IT & Law Consulting GmbH in Zug und Luzern. Nach dem Studium der Rechts-

wissenschaften in Graz (Österreich) spezialisierte sie sich auf rechtliche Themen an der Schnittstelle zwischen Informationstechnologie und Recht. Sie unterstützt Unternehmen bei der Ausarbeitung von Verträgen im Informatikbereich und berät diese in rechtlichen Fragestellungen, welche sich aus dem Einsatz oder der Entwicklung von Informationstechnologie ergeben. Maria Winkler ist zudem Dozentin für Informatikrecht an der Hochschule für Wirtschaft (HSLU) Luzern und unterrichtet Themen wie Urheberrecht, Datenschutzrecht und Recht im Internet. Kontakt: maria.winkler@itandlaw.ch oder www.itandlaw.ch

## VON MARIA WINKLER

**B**iometrische Daten gelten grundsätzlich als Personendaten. Auch wenn mit biometrischen Zutrittskontrollsystemen keine Rohdaten (zum Beispiel das Originalabbild eines Fingerabdrucks) sondern nur Templates (extrahierte Merkmale) gespeichert werden, ist es möglich, die Person durch einen Abgleich mit einem aktuell präsentierten biometrischen Merkmal zu bestimmen. Sobald die betroffene Person bestimmbar ist, handelt es sich um Personendaten, weshalb die datenschutzrechtlichen Vorgaben zu beachten sind. Plant ein Unternehmen, ein biometrisches Zutrittskontrollsystem einzuführen, ist es daher gut beraten, sich rechtzeitig mit den datenschutzrechtlichen Vorgaben auseinanderzusetzen.

## Auswahl des biometrischen Systems

Es sollte bereits bei der Auswahl und der Ausgestaltung auf die Datensparsamkeit des Zutrittskontrollsystems geachtet werden. Der beabsichtigte Verwendungszweck ist dabei ausschlaggebend dafür, wie viele Personendaten ein biometrisches Zutrittskontrollsystem speichern und bearbeiten darf, um den datenschutzrechtlichen Ansprüchen zu genügen. So müssen beispielsweise nur wenige Daten erhoben werden, um kontrollieren zu können, ob eine Person berechnigt ist, ein Gebäude zu betreten. Muss hingegen nachgewiesen werden können, welche Person sich zu welchem Zeitpunkt und wie lang in einem geschützten Bereich aufgehalten hat, dann sind zusätzlich zu den biometrischen



**Biometrische Daten müssen in einem absolut sicheren Umfeld aufbewahrt werden.**

(Bild: shutterstock)

Merkmale auch der Name, das Datum, die Zeit und eventuell weitere Informationen zu erheben.

### **Transparenz gegenüber betroffenen Personen**

Seit dem Inkrafttreten der revidierten Bestimmungen des Datenschutzgesetzes in der Schweiz (01. Januar 2008) sind die Anforderungen an die Transparenz der Datenbearbeitung gestiegen. Die betroffenen Personen müssen wissen, dass biometrische Daten über sie erhoben werden und zu welchem Zweck. Muss die betroffene Person an der Beschaffung der biometrischen Daten zwingend mitwirken (beispielsweise bei der Abgabe des Fingerabdrucks), dann ist die Erhebung für sie klar erkennbar. Diesen Systemen ist daher der Vorzug zu geben gegenüber Systemen, welche eine Erhebung der Daten ohne Wissen und Mitwirkung der betroffenen Person ermöglichen. Darüber hinaus müssen die betroffenen Personen darüber aufgeklärt werden, zu welchem Zweck die Daten benötigt werden.

### **Verhältnismässigkeit und Zweckbindung**

Damit ein biometrisches Zutrittskontrollsystem den gesetzlichen Anforderungen an eine zweckmässige und verhältnismässige Datenbearbeitung entspricht, muss sichergestellt werden, dass nur die objektiv für den angestrebten Verwendungszweck tatsächlich benötigten Daten erhoben und bearbeitet werden. Zudem sollte das System so ausgestaltet sein, dass ein Auslesen der Daten und die Verwendung zu einem anderen Zweck verunmöglicht wird. Nicht mehr benötigte Daten müssen rechtzeitig und zudem sicher gelöscht werden.

### **Sicherheit**

Die Tatsache, dass biometrische Merkmale mit der betroffenen Person untrennbar und nicht veränderbar verbunden sind und

daher nicht vergessen werden können, wird häufig als einer der grössten Vorteile gegenüber der Benutzung von Passwörtern genannt. Gerade die Unveränderbarkeit der biometrischen Daten birgt aber auch eine grosse Gefahr für die betroffene Person. Werden die Daten gestohlen oder gehen sie verloren, dann können sie nicht ersetzt werden. Dem Sicherheitsaspekt ist daher für die Verwendung biometrischer Zutrittskontrollsysteme besondere Beachtung zu schenken und es ist zu gewährleisten, dass die biometrischen Daten in einem absolut sicheren Umfeld aufbewahrt werden.

### **Persönlichkeitsschutz für den Einsatz von Biometrie**

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) hat zur Frage, unter welche Bedingungen biometrische Systeme im Privatbereich verhältnismässig verwendet werden, im Zusammenhang mit der Zutrittskontrolle der Sport- und Freizeitanlagen des KSS Schaffhausen (Schweiz) Stellung genommen.

Gemäss EDÖB ist der Persönlichkeitsschutz dann am ehesten gewahrt, wenn

- ▶ die biometrischen Daten auf einem Speichermedium, das sich in der alleinigen Kontrolle der betroffenen Person befindet, auslesesicher gespeichert werden
- ▶ die betroffene Person jeden Zugriff auf die Daten explizit und bewusst freigeben muss
- ▶ die Verifizierung der Identität ausschliesslich auf diesem Sicherheitsmedium stattfindet, sodass die biometrischen Da-

ten zu keinem Zeitpunkt die gesicherte Umgebung des Mediums und die Kontrolle der betroffenen Person verlassen.

Die gesamte Stellungnahme kann auf der Website des EDÖB unter [www.edoeb.admin.ch](http://www.edoeb.admin.ch) abgerufen werden.

### **Fazit**

Die Kontrolle des Zutritts zu Räumen und Gebäuden unter Verwendung biometrischer Merkmale wie dem Fingerabdruck hat gegenüber anderen Systemen wesentliche Vorteile. Im Gegensatz zu Passwörtern, welche häufig vergessen werden, sind biometrische Merkmale mit der betroffenen Person untrennbar verbunden. Zudem kann die berechnete Person eindeutig identifiziert werden, weil die Merkmale sich nicht verändern und daher einmalig sind.

Gerade deshalb handelt es sich aber bei den biometrischen Daten um sehr sensible Informationen. Der erfolgreiche Einsatz biometrischer Zutrittskontrollsysteme hängt daher wesentlich davon ab, dass die Personen, deren Daten erhoben und bearbeitet werden, darauf vertrauen, dass mit ihren Daten sorgfältig umgegangen wird. Die transparente Information über die bearbeiteten Daten sowie über die Funktionsweise des Systems schafft das nötige Vertrauen der betroffenen Personen. Wenn die Anforderungen des Datenschutzes bereits bei der Anschaffung eines biometrischen Zutrittskontrollsystems berücksichtigt werden, dann können unnötige Risiken und kostenintensive Korrekturen am System verhindert werden. ■



**Das Vergessen von Passwörtern gehört dank der Biometrie der Vergangenheit an.** (Bild: shutterstock)