Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Datenspeicherung bei Verifizierungssystemen

Ausgangslage

Es ist allgemein anerkannt, dass die mehrfache Verwendung legitimierender Merkmale ein Sicherheitsrisiko darstellt und daher vermieden werden soll; so wird z.B. dringend empfohlen, für jede Bankkarte einen anderen PIN zu verwenden und ihn regelmässig zu wechseln. Die Verwendung biometrischer Erkennungssysteme läuft dieser Empfehlung diametral entgegen: Zum einen steht pro Charakteristikum nur eine begrenzte Anzahl Proben zu Verfügung (z.B. hat man nur zehn Finger oder nur zwei Augen), und zum anderen fokussieren sich die gängigen Systeme auf dieselben Merkmale (eine überwiegende Mehrheit der Systeme verwendet Fingerabdrücke). Eine grosse Variation oder ein regelmässiger Wechsel ist damit nicht möglich. Deshalb müssen an die Sicherheit im Umgang mit biometrischen Daten besonders hohe Anforderungen gestellt werden.

Die Wahl des Speicherortes biometrischer Daten ist aus datenschutzrechtlicher Sicht von grosser Wichtigkeit. Die zentrale Speicherung solcher Daten führt zu einem grösseren Eingriff in die Persönlichkeitsrechte der betroffenen Personen. Solcherart gespeicherte Daten könnten auch ohne Zutun der Betroffenen verwendet werden, womit diese das Recht auf informationelle Selbstbestimmung in diesem Bereich nicht mehr ausüben können. Bei zentral gespeicherten biometrischen Daten steigt das Risiko eines Missbrauchs, da einerseits grosse Mengen solcher Daten vorliegen können und andererseits die betroffenen Personen keinerlei Kontrolle über sie haben.

Zwei Vorgänge werden unterschieden: die Identifizierung und die Verifizierung. Bei biometrischen **Identifizierungssystemen** wird geprüft, wer eine anwesende Person ist (z.B. ob eine bestimmte Person die in der Mitarbeiterdatenbank gespeicherte Frau XY ist). Hier wird also mit einem 1:n-Vergleich die Identität einer Person festgestellt, so dass eine zentrale Datenbank notwendig ist. Anders verhält es sich bei der Verifizierung: Werden die biometrischen Daten mit dem Ziel bearbeitet, die behauptete Identität einer Person zu **verifizieren** (z.B. ob eine bestimmte Person tatsächlich Inhaberin der vorgewiesenen Abonnementskarte ist), besteht für eine zentrale Speicherung der Daten keine Notwendigkeit. Bei solchen Verifizierungsprozessen findet ein Vergleich zwischen einer biometrischen Probe (z.B. dem ans Lesegerät gehaltenen Finger) und einem bestimmten Referenzdatum (z.B. dem auf einer Karte gespeicherten Referenzfingerabdruck) statt, also ein 1:1 Vergleich. Daher sollten hier die Daten aus Gründen der Verhältnismässigkeit und zur Garantie der informationellen Selbstbestimmung nur auf der Karte, also dezentral gespeichert werden.

Es können jedoch Gründe vorliegen, die eine **Dezentralisierung verunmöglichen** oder nur mit einem unverhältnismässig grossen Aufwand realisierbar machen. Soll ein Verifizierungssystem also mit zentral gespeicherten biometrischen Daten eingerichtet werden, ist den erhöhten Anforderungen an den Datenschutz anderweitig Rechnung zu tragen. Im Folgenden wird aufgezeigt, wie biometrische Daten bei Verifizierungssystemen datenschutzkonform gespeichert werden können. Andere, hier nicht vorgestellte Varianten sind denkbar, sofern die Anforderungen an den Datenschutz erfüllt werden.

Weitere Informationen zum Thema können unserem Leitfaden zu biometrischen Erkennungssystemen entnommen werden.

Feldeggweg 1, 3003 Bern
Tel. 058 463 74 84, Fax 058 465 99 96
www.edoeb.admin.ch

Allgemeine Anforderungen

Biometrische Rohdaten enthalten deutlich mehr Informationen über eine bestimmte Person als Templates (vgl. unseren Leitfaden zu biometrischen Erkennungssystemen), unter Umständen sogar besonders schützenswerte Personendaten (z.B. können gewisse Augenkrankheiten in einem Irisscan erkannt werden). Die Verwendung biometrischer Rohdaten greift daher regelmässig tiefer in die Persönlichkeitsrechte der betroffenen Personen ein als diejenige von Templates. Für den Einsatz in einem biometrischen Erkennungssystem reichen Letztere in der Regel aus. Der durch die Verwendung von Rohdaten verursachte tiefere Eingriff in die Persönlichkeitsrechte der Betroffenen ist daher unnötig und damit unverhältnismässig. Entsprechend müssen für biometrische Erkennungssysteme Templates anstelle von Rohdaten verwendet werden.

Bei der Verwendung biometrischer Daten ist der Datensicherheit besondere Bedeutung zuzumessen. Biometrische Daten können nicht nur besonders schützenswert sein, sondern sind auch dauerhaft mit einer Person verbunden und im Falle eines Missbrauchs nicht einfach zu ersetzen. Daher müssen gespeicherte biometrische Daten, unabhängig vom Speicherort, durch zusätzliche Massnahmen (z.B. Verschlüsselung) geschützt werden.

Systeme mit externem Datenträger

Die informationelle Selbstbestimmung kann am ehesten gewahrt werden, wenn Systeme mit externen Datenträgern eingesetzt werden, wie nachfolgend gezeigt wird.

Dezentralisierung

Die Dezentralisierung stellt die informationelle Selbstbestimmung der betroffenen Person am besten sicher und ist daher zu bevorzugen. Hierbei werden die biometrischen Daten einzig auf einem externen Datenträger, z.B. auf einer Smartcard, gespeichert und befinden sich damit in der ausschliesslichen Gewalt der betroffenen Person. Sie muss die Verwendung ihrer biometrischen Daten jedes Mal explizit und bewusst freigeben und weiss daher immer, wann sie verwendet werden. Wird gar ein System on Card verwendet (vgl. unseren Leitfaden zu biometrischen Erkennungssystemen), verlassen die biometrischen Daten den Herrschaftsbereich der betroffenen Person zu keinem Zeitpunkt, weshalb diese Variante den Persönlichkeitsschutz am besten sicherstellt.

Werden die biometrischen Daten ausschliesslich dezentral auf einem externen Datenträger gespeichert, der sich im Besitz der betroffenen Person befindet, und ist damit das informationelle Selbstbestimmungsrecht sichergestellt, können für das Erkennungssystem beliebige biometrische Charakteristika verwendet werden (Charakteristika mit oder ohne Spuren, vgl. unseren Leitfaden zu biometrischen Erkennungssystemen).

«Pseudodezentralisierung»

Bei dieser Variante werden die biometrischen Daten zwar zentral gespeichert. Der Bezug zu weiteren Personendaten ist jedoch nur mit Hilfe eines für jede Person unterschiedlichen Zuordnungscodes herstellbar. Dieser Zuordnungscode wird auf einem externen Datenträger gespeichert, ohne dass ihn der Systembetreiber kennt. Er kann daher nicht sagen, wem die bei ihm zentral gespeicherten biometrischen Daten konkret zuzuordnen sind. Eine Zuordnung ist nur dann möglich, wenn die fragliche Person anwesend ist und die Karte einsetzt.

Sobald die Karte im Lesegerät eingelesen wird, kann in der Datenbank das dazugehörige Template geladen und die Verbindung zu weiteren Daten über die fragliche Person (z.B. Personalien, Berechtigungen etc.) hergestellt werden. Die Identität der Person wird aufgrund des präsentierten biometrischen Merkmals verifiziert und die Verbindung zwischen Template und weiteren Personendaten anschliessend sofort unterbrochen. Selbstverständlich dürfen die Zugriffe auf die verschiedenen Datensets nicht so protokolliert werden, dass eine Zuordnung, z.B. aufgrund übereinstimmender Zeitstempel, wieder möglich wird.

Diese Variante hat gegenüber der Dezentralisierung den Vorteil, dass die auf dem externen Datenträger gespeicherte Datei (also der Zuordnungscode) deutlich kleiner ist als ein Template. Damit kann einerseits die Speicherkapazität des externen Speichers verringert, andererseits aber auch die Schnelligkeit des Systems erhöht werden.

Da bei der Pseudodezentralisierung die biometrischen Daten zentral gespeichert werden, ist das informationelle Selbstbestimmungsrecht der betroffenen Personen entsprechend eingeschränkt. Zudem besteht ein erhöhtes Risiko des Datenmissbrauchs. Aus diesem Grund sind bei dieser Variante biometrische Charakteristika ohne Spuren (vgl. unseren Leitfaden zu biometrischen Erkennungssystemen) zu bevorzugen.

Systeme ohne externen Datenträger

Zentralisierung

Möchte oder muss man auf den Einsatz externer Datenträger verzichten, so ist für ein biometrisches Erkennungssystem zwingend eine zentrale Speicherung notwendig. Wie bereits ausgeführt, sind die Risiken einer missbräuchlichen Datenbearbeitung bei einer zentralen Speicherung höher.

Da im zentralen Datenspeicher eine grosse Menge biometrischer Daten vorliegen, ist es nicht zuletzt für Dritte attraktiv, sich Zugang dazu zu verschaffen. Die Anforderungen an die allgemeine Datensicherheit sind bei solchen Systemen deshalb sehr hoch. Der Betreiber muss ausschliessen können, dass die Daten widerrechtlich ausgelesen werden könnten. Weiterführende Informationen zu den in diesem Bereich möglichen Sicherheitsmassnahmen entnehmen Sie unserem Leitfaden zu den technischen und organisatorischen Massnahmen.

Eine weitere Gefahr besteht in der Verknüpfbarkeit. Die biometrischen Daten lassen sich mit anderen Angaben der betroffenen Personen oder aber mit anderen biometrischen Systemen verknüpfen, bis hin zu einem Persönlichkeitsprofil. Im Bereich der Biometrie kann dies unabsehbare Konsequenzen haben – wenn bspw. verschiedene Zutrittsysteme mit demselben Fingerabdruck funktionieren, könnte nachvollzogen werden, wann sich eine bestimmte Person im Sportclub, wann in der Disco aufhält; so entstünde ein Bewegungsprofil – je öfter der Fingerabdruck eingesetzt wird, desto schlimmer wäre es, wenn das biometrische Rohdatum dazu abhanden käme. Daher dürfen biometrische Daten nur ohne Bezug zu weiteren Personendaten gespeichert werden. Mit anderen Worten müssen sie auf einem separaten Speicher abgelegt werden, auf dem weder die Personalien noch ein Pseudonym (bspw. Mitarbeiternummer) der betroffenen Personen gespeichert sind. Dieser Bezug darf für den Datenbearbeiter nicht herstellbar sein, weder durch eine Zuordnungsliste noch durch Zeitstempel oder dergleichen. Zudem darf der Datenspeicher über keinerlei Kommunikationsmöglichkeiten mit anderen Geräten verfügen – möglich wäre also bspw. ein Standalone-System zur Zugangskontrolle, das keine Anschlussmöglichkeiten hat, über die die biometrischen Daten ausgelesen werden könnten.

Bei der zentralen Speicherung biometrischer Daten wird das informationelle Selbstbestimmungsrecht stark eingeschränkt. Da für die Verwendung solcher Systeme keine externen Datenspeicher benötigt werden und bei der Prüfung einer Zugangsberechtigung einzig auf das biometrische Merkmal abgestellt wird, ist das Missbrauchsrisiko noch höher als bei der oben beschriebenen «Pseudodezentralisierung». Ist man erst einmal im Besitz der biometrischen Daten einer bestimmten Person, wäre es grundsätzlich einfach möglich, sich gegenüber dem System als diese auszugeben (Stichwort Identitätsdiebstahl), da die zusätzliche Legitimierung mittels Token entfällt. Daher dürfen bei biometrischen Zutrittssystemen mit zentraler Datenspeicherung ausschliesslich biometrische Charakteristika ohne Spuren zur Anwendung kommen. Diese Charakteristika (z.B. Finger- oder Handvenenmuster) können im Gegensatz zu denjenigen mit Spuren (z.B. Fingerabdruck) nicht ohne weiteres hinterlassen oder von aussen wahrgenommen werden (vgl. unseren Leitfaden zu biometrischen Erkennungssystemen [Link]). Dadurch lässt sich ausschliessen, dass diese Merkmale ohne das Wissen der betroffenen Person entnommen werden.

Dezentralisierung	**Pseudo-Dezentralisierung**	**Zentralisierung**
Biometrische Charakteristika **mit oder ohne Spuren** Biometrische Daten **dezentral** auf Smartcards gespeichert	Biometrische Charakteristika **mit oder ohne Spuren** Biometrische Daten **zentral** gespeichert **Bezug** zu weiteren Personendaten nur mit Einsatz einer **Karte** herstellbar	Nur biometrische Charakteristika **ohne Spuren** Biometrische Daten **zentral** gespeichert **Kein Bezug** zu weiteren Personendaten

Stand: Juli 2013