

**10th Symposium
on Privacy and Security**

Biometrie und Datenschutz:



Wird der Mensch maschinenlesbar?

Lic. iur. Beda Harb
Stellvertreter des Datenschutzbeauftragten
des Kantons Zürich

Lic. iur. Daniel Schmid
Beauftragter für Information und
Datenschutz des Kantons Solothurn





Inhalt

- Technik
- Verfassungsrechtliche
Rahmenbedingungen
- Datenschutzrechtliche
Anforderungen
- Folgerungen

2



Biometrie

- Biometrie: Messverfahren
- Biometrische Merkmale
 - Körpereigen
 - Einmaligkeit
 - Untrennbare Verknüpfung mit bestimmter Person



Biometrische Merkmale

- Physiologische (passive) Merkmale,
z.B. Fingerabdruck, Gesicht, Iris, Retina
- Verhaltensbasierte (aktive)
Charakteristika, z.B. Stimme,
Schrift / Unterschrift
- Physikalische Merkmale (DNA)



Biometrische Verfahren

- Erfassung des Merkmals mit Sensor (z.B. Kamera, Scanner, Mikrofon)
→ Entnahme Rohdaten (z.B. Foto, Videoaufnahme, Sprachaufnahme)
- Generierung eines Templates
- Ablage des Templates
- Erzeugung eines Prüfmusters
- Vergleich von Template und Prüfmuster



Biometrische Daten sind Personendaten (1)

- Definition „Personendaten“
 - Art. 3 Bst. a des eidgenössischen Datenschutzgesetzes (DSG):
„Alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen“
- Biometrische Merkmale, daraus erzeugte Rohdaten, Templates, sind ohne weiteren Personenbezug (z.B. Name) Personendaten!



Biometrische Daten sind Personendaten (2)

- Definition „besonders schützenswerte Personendaten“
 - Art. 3 Bst. c DSG: „Daten über:
 1. die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten,
 2. die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit,
 3. Massnahmen der sozialen Hilfe,
 4. Administrative oder strafrechtliche Verfolgungen und Sanktionen“



Biometrische Daten sind Personendaten (3)

- Qualifikation biometrischer Daten als besonders schützenswerte Personendaten, z.B.
 - Verwendung
 - Persönlichkeitsprofile
 - Soweit technisch möglich, eindeutige Rückschlüsse auf körperliche, charakterliche Eigenschaften, Gesundheit, Rasse / Ethnie
 - Besondere Gefahr einer Persönlichkeitsverletzung



Grundrechte

- Menschenwürde, Art. 7 Bundesverfassung (BV)
- Persönliche Freiheit, Art. 10 BV
- Privatsphäre und Recht auf informationelle Selbstbestimmung, Art. 13 BV
- Menschenwürde und Kerngehalt Grundrechte decken sich



Menschenwürde

- Menschenwürde im besonderen:
 - Definition „Menschenwürde“ Art. 7 BV:
„Die Würde des Menschen ist zu achten und zu schützen“
 - Kernaussage: Mensch darf nicht als „Objekt“, „Nummer“, „Ware“ behandelt werden!
 - Menschenwürde darf nicht eingeschränkt werden, selbst nicht bei Krieg, Gefahren für das Überleben des Staates



Menschenwürde und Biometrie

- „Menschenunwürdiger“ Einsatz biometrischer Verfahren, Rohdaten, Templates, z.B.
 - Flächendeckender Einsatz als „Personenidentifikator“
 - Einsatz in zentraler Datenbank, Daten über alle EinwohnerInnen, ohne enge Zweckbindung, auf unbestimmte Zeit, keine Zugriffsbeschränkungen



Verfassungsrechtliche Folgerungen

- Biometrie darf nicht zu einer breiten Identifikation / Verifikation von uns Menschen führen (Masseneinsatz)
- Suggestierte Einfachheit, Bequemlichkeit bildet keine Rechtfertigung für eine Aufgabe der Privatheit, Anonymität in weiten Teilen unseres täglichen Lebens



Datenschutzrechtliche Anforderungen

- Biometrische Daten – Rohdaten und Templates - sind Personendaten
- Wie jede andere Datenbearbeitung muss der Einsatz eines biometrischen Systems durch ein staatliches Organ den datenschutzrechtlichen Grundsätzen genügen.
- Beispiel: Kommunales Schwimmbad



Rechtsgrundlage

- Datenbearbeitung durch staatliche Organe bedarf einer gesetzlichen Grundlage
- Biometrische Daten unter bestimmten Voraussetzungen besonders schützenswerte Personendaten
- Gesichtsbild oder Fingerabdruck zur Verifikation der AbonnentInnen nicht zwingend in Gesetz im formellen Sinn



Verhältnismässigkeit (1)

- Das Bearbeiten von Personendaten muss für die Erfüllung der Aufgabe geeignet und erforderlich sein.
- Biometrie darf nur eingesetzt werden, soweit ein Identifizierungsbedarf konkret begründet ist.
- Verwendung Gesichtsbild oder Fingerprint-Template im Beispiel Schwimmbad verhältnismässig



Verhältnismässigkeit (2)

- Für die Autorisierung beim Schwimmbad-Eintritt genügt ein Gesichtsbild oder ein Fingerprint-Template
- Personenbezogene Randdaten: Maschinenlesbar



Zweckbindung (1)

- Daten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, der aus den Umständen ersichtlich ist oder der gesetzlich vorgesehen wird.
- Zweck eng zu fassen
- Technische Lösung ist so auszugestalten, dass Zweck der Datenbearbeitung erreicht wird, Änderungen des Bearbeitungszweckes aber ausgeschlossen werden



Zweckbindung (2)

- Datenbearbeitung möglichst in Nutzersphäre
- Template auf Smartcard und nicht in Datenbank
- Keine Gewinnung von Zusatzinformationen
- Soweit und so früh wie möglich Templates verwenden
- Keine Wiederherstellung der Rohdaten aus Template



Richtigkeit

- Personendaten müssen richtig und, soweit es der Zweck des Bearbeitens verlangt, vollständig sein.
- Verfahren einsetzen, das eine nahezu 100%-ige Wahrscheinlichkeit der Verifikation erlaubt
- Alternativszenario für Personen, die nicht eingelernt werden können



Sicherheit

- Daten müssen durch angemessene organisatorische und technische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.
- Sicherheitskonzept
- Hohe Ausfallsicherheit gewährleisten; Risiko des Ausfalles des biometrischen Systems liegt bei der Betreiberin und darf nicht auf die nutzenden Personen übertragen werden



Transparenz

- Personendaten sind in der Regel bei der betroffenen Person zu beschaffen.
- Biometrischen Daten dürfen ohne Wissen und Willen der betroffenen Person nicht erfasst oder übermittelt werden.
- Kombiniertes Einsatz mit Funktechnologie führt zu neuen Fragestellungen



Verantwortlichkeit

- Bearbeitendes Organ ist für die Einhaltung der datenschutzrechtlichen Anforderungen verantwortlich.
- Die Gemeinde als Betreiberin des Schwimmbades kann Ihre Verantwortung nicht auf Dritte übertragen.



Rechte der betroffenen Person

- Datenschutzrechtliche Auskunfts- Einsichts- und Berichtigungsrechte sowie Rechte zur Unterlassung, Feststellung oder Beseitigung rechtswidriger Bearbeitung von Personendaten
- Sicherzustellen, dass betroffene Personen die ihr zustehenden Rechte uneingeschränkt ausüben können.



Folgerungen (1)

- Kein verfassungswidriger Einsatz biometrischer Verfahren
- Biometrie darf nicht zu einer breiten Identifikation / Verifikation von uns Menschen führen (Masseneinsatz)
- Suggestierte Einfachheit, Bequemlichkeit bildet keine Rechtfertigung für eine Aufgabe der Privatheit, Anonymität in weiten Teilen unseres täglichen Lebens



Folgerungen (2)

- Technische Lösung ist auf die datenschutzrechtlichen Anforderungen auszurichten.
- Datenschutzkonforme Lösung möglich
- Datenschutzrechtliche Aspekte bereits bei Evaluation und Planung des Systems zu berücksichtigen
- Akzeptanz