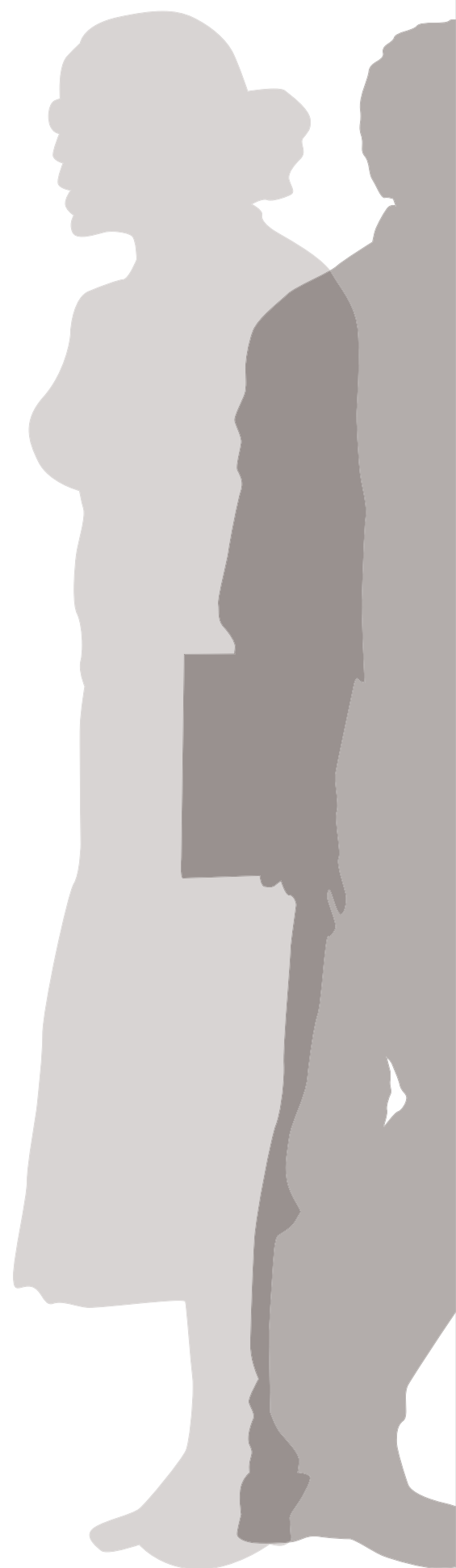




Leitfaden zur datenschutzrechtlichen Beurteilung von biometrischen Verfahren

(mit Checkliste für Projekte im öffentlich-rechtlichen Bereich)





1.	Vorbemerkungen	2
2.	Kurzfassung	3
3.	Begriffe und technische Aspekte	4
3.1.	Begriffe	
3.1.1	Biometrie	
3.1.2	Biometrische Merkmale	
3.1.3	Biometrische Verfahren	
3.1.4	Funktionen des biometrischen Verfahrens	5
3.1.5	Fehlerbegriffe	6
3.1.6	Zusatzinformationen	
3.1.7	Automatisierte Verfahren, Randdaten	
3.2.	Sicherheit bei der Bearbeitung biometrischer Daten	
3.3.	Standardisierung	7
3.4.	Technische Entwicklung als Begründung für Biometrie	8
4.	Rechtliche Rahmenbedingungen	9
4.1.	Biometrische Daten sind Personendaten	
4.2.	Verfassungsrechtliche Rahmenbedingungen	
4.2.1	Betroffene Grundrechte	
4.2.2	Einschränkung der Grundrechte	10
4.2.3	Verletzung der Menschenwürde	
4.2.4	Verletzung des individuellen Selbstbestimmungsrechts	11
4.3.	Datenschutzrechtliche Rahmenbedingungen	
4.3.1	Einhaltung der allgemeinen datenschutzrechtlichen Grundsätze	
4.3.2	Rechtsgrundlage	
4.3.3	Zweckbindung	
4.3.4	Verhältnismässigkeit	12
4.3.5	Transparenz	13
4.3.6	Richtigkeit	
4.3.7	Kontrollrechte der betroffenen Person	
4.3.8	Datensicherheit	
4.3.9	Verantwortung	
5.	Anwendungsbeispiele	14
5.1.	Anwendungen durch staatliche Organe in der Schweiz	
5.2.	Anwendungen durch staatliche Organe in der EU	
5.3.	Anwendungen durch staatliche Organe im übrigen Ausland	
6.	Datenschutzrechtliche Forderungen	15
Anhang 1:	Übersicht über biometrische Merkmale und Verfahren	16
Anhang 2:	Checkliste zur datenschutzrechtlichen Beurteilung biometrischer Projekte im öffentlich-rechtlichen Bereich	18
Anhang 3:	Literaturhinweise	21
	Adressen	24

Vorbemerkungen

Mit dem vorliegenden Leitfaden wird beabsichtigt, den Mitgliedern der Vereinigung und dem interessierten Publikum einen ersten Einblick in die Thematik der Biometrie zu gewähren und dem Leser oder der Leserin die datenschutzrechtlich relevanten Fragen aufzuzeigen. Dabei verfolgt die Vereinigung keine wissenschaftlichen Ziele, sondern es geht lediglich darum, ein Hilfsmittel für die Beurteilung von biometrischen Verfahren zur Verfügung zu stellen. Um die Lesbarkeit des Leitfadens zu vereinfachen, wurde auf Fussnoten oder Verweise verzichtet. Auch Zitate sind nicht als solche gekennzeichnet. Das vorliegende Papier bezweckt nicht die Beantwortung sämtlicher offener Fragen zu einem Thema, welches einer sehr raschen Entwicklung untersteht. Für eine vertiefte Auseinandersetzung wird auf die Literaturhinweise im Anhang 3 verwiesen.

Der Text des Leitfadens gewährt einen kurzen Überblick über die Biometrie, der Anhang 1 fasst die biometrischen Merkmale und Verfahren zusammen und der Anhang 2 soll dem Leser oder der Leserin eine Checkliste bieten, nach welcher ein biometrisches Verfahren datenschutzrechtlich beurteilt werden kann.

Im Leitfaden werden beispielhaft lediglich die Gesetzesbestimmungen des Bundes erwähnt, insbesondere das Bundesgesetz über den Datenschutz vom 19. Juni 1992 (SR 235.1; nachfolgend DSG). Bei biometrischen Verfahren, die durch kantonale Organe eingesetzt werden, sind die entsprechenden kantonalen Datenschutzgesetze zu berücksichtigen, die im Einzelnen von der Regelung des Bundes abweichen können.

Der Leitfaden bezieht Positionen, die nicht zwingend die Meinung sämtlicher Vereinsmitglieder widerspiegeln.

Spezieller Dank gebührt Herrn Daniel Schmid, Informations- und Datenschutzbeauftragter des Kantons Solothurn, sowie Herrn Beda Harb, Stellvertreter des Datenschutzbeauftragten des Kantons Zürich, welche die erste Fassung des vorliegenden Leitfadens verfasst haben.

Biometrische Merkmale sind einmalige, spezielle körpereigene Kennzeichen einer Person, die – zumindest theoretisch - immer und überall eindeutig mit nahezu 100%iger Sicherheit nur dieser einen Person zugeordnet werden können. Sie werden digital erfasst und verglichen.

Biometrische Daten (Rohdaten und Templates) sind Personendaten, oft sogar besonders schützenswerte (z.B. auf Grund ihrer Verwendung in den Bereichen Gesundheit, Soziale Hilfe/Sozialversicherungen, Strafverfahren).

Biometrische Verfahren tangieren per se die Menschenwürde nicht. Diese wird aber immer dann verletzt, wenn biometrische Verfahren - auch Kombination mit anderen technischen Anwendungen - dazu führen, dass der Mensch nur noch als Objekt, quasi wie eine Nummer, eine Ware, behandelt wird.

Für biometrische Anwendungen sind die datenschutzrechtlichen Rahmenbedingungen – Rechtsgrundlage, Zweckbindung, Verhältnismässigkeit, Transparenz, Richtigkeit, Rechte der betroffenen Personen, Datensicherheit – einzuhalten. Ansonsten ist von einer Verletzung der informationellen Selbstbestimmung bzw. der persönlichen Freiheit auszugehen.

Besonderes Augenmerk ist darauf zu richten, dass die bearbeiteten Daten im Herrschaftsbereich der betroffenen Person bleiben und dass zweckwidrige Datenbearbeitungen ausgeschlossen werden.

3.1

Begriffe

3.1.1

Biometrie

Biometrie ist die automatisierte Messung von natürlichen, charakteristischen, physiologischen oder verhaltenstypischen Merkmalen von Menschen zum Zweck der Unterscheidung von anderen Personen.

3.1.2

Biometrische Merkmale

Biometrische Merkmale sind spezielle körpereigene Kennzeichen einer Person, die – zumindest theoretisch – immer und überall eindeutig mit nahezu 100%iger Sicherheit nur dieser einen Person zugeordnet werden können.

Biometrische Merkmale lassen sich derzeit nur ausnahmsweise und mit erheblichem Aufwand verändern (z.B. plastische Gesichtschirurgie). Aus ihnen gewonnene biometrische Daten sind deshalb nicht nur personenbezogen, sondern personengebunden. Die daraus gewonnenen Rohdaten sind – gemäss Begriffsdefinition – für jeden Menschen einmalig. Eine «Neuvergabe», ein «Update» oder eine Weitergabe, eine Veränderung der Bindung der Daten an die Person, ist in der Regel nicht möglich. Dies ist bei einem Passwort (Wissen) oder einem Schlüssel (Besitz) anders.

Die Merkmale lassen sich in drei Gruppen unterteilen: Physiologische (passive), verhaltenstypische (aktive) und physikalische Charakteristika. Die wichtigsten biometrischen Merkmale sind derzeit das Gesicht, der Fingerabdruck sowie die Iris (siehe auch Anhang 1). Geschlecht, Grösse und Augenfarbe sind zwar ebenfalls körpereigene Kennzeichen einer Person, jedoch nicht unverwechselbar und fallen deshalb als biometrische Merkmale weg.

Physiologische und verhaltenstypische Merkmale sind bei der grossen Mehrheit der Menschen vorhanden und messbar, jedoch nicht bei allen. Beispielsweise wird davon ausgegangen, dass rund zwei Prozent aller Menschen für die biometrische Verwendung ihres Fingerabdruckes nicht geeignet sind (Geburtsgebrechen, Amputation, Verätzung, Verletzung, Schwierigkeiten bei der Erfassung). Hochgerechnet bedeutet dies, dass in der Schweiz bei rund 150'000 Personen ein Vergleich ihrer Fingerabdrücke nicht möglich sein dürfte. Im Pilotbetrieb der Iris-Erkennung am Flughafen Frankfurt konnten 1,3 Prozent der Personen nicht eingelernt werden.

3.1.3

Biometrische Verfahren

Mittels eines biometrischen Verfahrens soll durch eine geeignete Auswahl biometrischer Merkmale eine eindeutige Zuordnung zu einem bestimmten Menschen erreicht werden.

Biometrische Verfahren sind nicht neu: Die Unterschrift und die persönliche Gesichtskontrolle mit und ohne Vergleich mit einer Fotografie werden seit langem eingesetzt; in Strafverfahren spielen Fingerabdrücke seit Jahrzehnten eine wichtige Rolle. Neu ist die digitale Erfassung und Auswertung von biometrischen Merkmalen mit Hilfe leistungsfähiger Systeme (Sensoren, Datenverarbeitung).



Ein biometrisches Verfahren läuft wie folgt ab:

1. Erfassung des Merkmals mit einem Sensor (z.B. Kamera, Mikrofon, Tastatur, Spezi­alsensor zur Aufnahme von Gerüchen oder Fingerabdrücken): Entnahme eines **elektronischen Abdruckes (biometrische Rohdaten)** wie Foto, Sprachaufnahme, Videoaufnahme).
2. Im biometrischen Verfahren wird ein spezielles Mustergenerierungs- oder Muster­erkennungsverfahren eingesetzt und aus dem Merkmal **ein Muster (Template)** des Abdrucks des personengebundenen Merkmals generiert (Feature Extraction). Dazu wird ein spezieller **Algorithmus** eingesetzt.
3. Das erzeugte Template wird abgelegt.
4. Ein auf dieselbe Weise erzeugtes Prüfmuster wird auf Übereinstimmung mit dem abgelegten Template oder einer Vielzahl von Mustern geprüft (Template Matching). Aus Rohdaten lässt sich jederzeit ein neues Template generieren. Es ist sicher­zustellen, dass der eingesetzte Algorithmus eine Wiederherstellung der Rohdaten aus dem Template nicht zulässt.

Auf einer Speichereinheit von 1 GB können Templates von Gesichtsbild und allen Fingerabdrücken von rund 100'000 Personen abgelegt werden (Template Fingerprint ca. 500 Bytes, Template des Gesichtsbildes ca. 2,5 KB). Die Rohdaten benötigen ein Vielfaches an Speicherplatz.

Das Template enthält in der Regel weniger Informationen als Rohdaten. Dement­sprechend sind die Folgen eines Missbrauchs oder einer Zweckentfremdung für die betroffene Person weniger einschneidend, weshalb die Ablage/Speicherung von Templates zu bevorzugen ist (Risikominimierung).

3.1.4

Funktionen des biometrischen Verfahrens

Verifikation (1:1-Vergleich oder «one-to-one matching»): Die Eingangsdaten werden mit Referenzdaten der Person verglichen, als die sich der Nutzer ausgibt, um deren Identität zu bestätigen. Ziel ist die Bestätigung resp. Nichtbestätigung der geltend gemachten Identität.

Identifikation (1:n-Vergleich oder «one-to-many matching»): Vergleich der Eingangs­daten mit den gespeicherten Referenzdaten vieler Individuen. Ziel ist die Feststellung der Identität einer Person; Personen werden aus einer Masse von anderen Personen erkannt.

Authentifikation/Authentifizierung: Bezeugung der Echtheit (z.T. wird Authentifikation der Verifikation gleichgestellt).

Authentisierungsverfahren: Wissen (Passwort, PIN), Besitz (Chipkarte, Schlüssel), Können (Unterschrift) oder Sein (Nutzer selbst: Biometrisches Merkmal) werden geprüft.

Autorisierung: Ermächtigung, Bevollmächtigung. Nach erfolgreicher Authenti­fikation (Verifikation oder Identifikation) wird eine Person ermächtigt, einen bestimmten Dienst zu nutzen oder eine Handlung vorzunehmen.

3.1.5

Fehlerbegriffe

Die Sicherheit von biometrischen Verfahren hängt von Wahrscheinlichkeiten ab, die Verfahren müssen kalibriert werden. Eine 100%ige Sicherheit gibt es nicht. Zwei Templates stimmen bei derselben Person kaum oder nie 100%ig überein: Wärme, Kälte, Stimmungen, Alterung, Tätigkeiten usw. führen zu leichten Merkmalsveränderungen. Dazu kommen Messunterschiede. Viele Templates sind deshalb extrem ähnlich; beinah biometrische Zwillinge müssen jedoch als solche erkannt werden.

False Rejection Rate (FRR): Anteil der falsch zurückgewiesenen Nutzer;

False Acceptance Rate (FAR): Anteil der fälschlich vom System zugelassenen Personen;

Equal Error Rate (ERR): FRR und FAR sind voneinander abhängig: Steigt die eine, sinkt die andere;

Threshold: Grenzwert, ab dem ein Ergebnis als akzeptabel klassiert werden kann (die Festlegung des zulässigen Grenzwertes ist eine sehr heikle Frage, die nicht nur der Technik überlassen werden darf);

Failure to enrol rate (FER): Prozentsatz der Personen, welche auf dem System nicht eingelernt werden können (die über entsprechendes biometrisches Merkmal nicht verfügen) oder die Schwierigkeiten bei der Erfassung des Merkmals haben (z.B. infolge Lähmung oder Grösse den Fingerprint-Scanner nicht erreichen können).

3.1.6

Zusatzinformationen

Die von den Sensoren erfassten Rohdaten enthalten in jedem Fall viel mehr Informationen als das daraus gewonnene Template: Bereits aus einem Gesichtsbild können Zusatzinformationen wie Hinweise auf Geschlecht, Alter, Ethnie, Aussehen, Stimmung, Krankheiten gewonnen werden. Aus physikalischen Merkmalen können bereits heute eindeutige besonders schützenswerte Zusatzinformationen gewonnen werden (u.a. genetische Informationen). Aus gespeicherten Rohdaten können jederzeit Zusatzinformationen gewonnen werden. Auch deswegen ist die Ablage/Speicherung von Templates zu bevorzugen.

3.1.7

Automatisierte Verfahren, Randdaten

Das Vorzeigen eines Ausweises und der manuelle Bildvergleich erfordert den Einsatz personeller Ressourcen und bedingt Entscheidungen durch Menschen. Die Registrierung des Vorzeigens und der Entscheidung erfordert einen erheblichen Zusatzaufwand. Biometrische Verfahren werden dagegen automatisiert durchgeführt; die Erstellung und der elektronische Vergleich von Rohdaten oder Templates erfolgt ohne personelle Ressourcen und menschliche Entscheidungen und kann leicht automatisiert aufgezeichnet werden (Randdaten, Logfiles). Werden Randdaten personenbezogen abgelegt, lassen sich auf einfache Art Bewegungsprofile erstellen; die Verknüpfung mit Zusatzdaten erlaubt die Erstellung von Persönlichkeitsprofilen.

3.2

Sicherheit bei der Bearbeitung biometrischer Daten

Wie bei der Bearbeitung von anderen Personendaten sind in biometrischen Verfahren entsprechende Sicherheitsmassnahmen zu ergreifen (Verschlüsselung, Schutz vor Manipulation an Hard-/Software und Daten, Schutz bei der Erfassung und Bearbeitung, Digitale Signatur, Zugriffs- und Zutrittsrechte).

Die technische Absicherung des biometrischen Verfahrens allein genügt jedoch nicht. Weitere Sicherheitsmassnahmen sind erforderlich:

- Verschiedene biometrische Merkmale können auch ohne Wissen/Willen der betroffenen Person erfasst werden (z.B. Videoaufnahme von Ferne, Fingerabdruck im Schlaf usw.).
- Wie bei Passwörtern (Wissen) und Schlüsseln (Besitz) stellt sich die Problematik der erzwungenen Authentisierung.

Um die Überlistung des Erfassungsvorganges («Gummifinger», Foto einer fremden Iris vor Auge) zu erschweren, ist es erforderlich, zu erkennen, ob das Merkmal Teil einer lebenden Person ist. Bei sicherheitskritischen Anwendungen wird die zusätzliche Verwendung einer Smartcard oder eines Tokens (Besitz) sowie die Eingabe eines Passwortes (Wissen) häufig unumgänglich sein. Mehrere biometrische Merkmale können auch kombiniert eingesetzt werden.

Von entscheidender Bedeutung sind die Massnahmen, welche die Reduktion der Fehlerrate erlauben (siehe vorstehend Ziff. 3.1.5) sowie die Massnahmen, welche einer von einem Fehler betroffenen Person zur Verfügung stehen, um negative Folgen eines allfälligen Fehlers abzuwenden (Kontrollrechte bzw. menschliche «over-ruling» Mechanismen). Liegt der definitive Entscheid bei der Maschine und ist der Mensch nicht in der Lage diese zu überstimmen, können automatisierte Entscheide tragische Folgen haben.

3.3

Standardisierung

Mit der Standardisierung bei der Erfassung von Rohdaten und der Erstellung von Templates sind eine Reihe von Problemstellungen verbunden. Einerseits sind Standardisierungen häufig wirtschaftlich sinnvoll und für den Abgleich von Templates unabdingbar. Andererseits ist für eine Standardisierung die ganze oder teilweise Offenlegung der Vorgehensweise bei der Erfassung der Rohdaten und der Erstellung der Templates nötig. Die Offenlegung und Transparenz fördert das Vertrauen, erleichtert aber auch Missbräuche.

Zudem kann eine weit gehende Standardisierung zu einer problematischen Monokultur führen. Es besteht die Gefahr, dass mit dem gleichen Algorithmus erzeugte Templates miteinander verglichen werden können; die Änderung des ursprünglichen Verwendungszweckes der Daten wird dadurch erleichtert.

Für den Einsatz biometrischer Daten in international gültigen Ausweispapieren ist eine international kompatible Identifikationsinfrastruktur aufzubauen. Diese Infrastruktur wird jedoch nicht nur in Ländern eingesetzt, in welchen Bürgerrechte geachtet werden und die über ein hohes Datenschutzniveau verfügen. Entsprechende Missbräuche können nicht ausgeschlossen werden. Dasselbe gilt für den Austausch biometrischer Daten in international geführten Datenbanken.

3.4

Technische Entwicklung als Begründung für Biometrie

Die technische Entwicklung ist rasant. Dabei ist es immer verlockend, das Kostengünstige und technisch Machbare zu realisieren, ohne das angewendete Verfahren rechtlich zu hinterfragen.

Vor wenigen Jahren war es für Privatanwender unmöglich oder mindestens unbezahlbar, ein digitales Bild einer Person herzustellen, zu besitzen oder zu bearbeiten. Bereits heute ist jedoch Spracherkennung oder digitaler Bildvergleich auf jedem PC möglich. Sensoren aller Art werden im Fachhandel und in Warenhäusern angeboten. Private Labors führen Vaterschaftstests für unter Fr. 1000.– durch. In USB-Memory-Sticks eingebaute Fingerprint-Sensoren werden für Fr. 100.– angeboten, inklusive Software zum Abgleich. Erste Laptops grosser Hersteller werden serienmässig mit Fingerprint-Sensor ausgeliefert.

Es ist davon auszugehen, dass diese Entwicklung rasch fortschreiten wird. Biometrische Verfahren sind bereits heute Allgemeingut geworden. Die technische Entwicklung beschränkt sich zudem nicht auf biometrische Verfahren. RFID, Funk- und Ortungstechnologie können zusammen mit Biometrie eingesetzt werden.

Eine reine technische oder finanzielle Begründung für die Einführung eines biometrischen Verfahrens ist ungenügend. Im Rechtsstaat misst sich die Zulässigkeit immer an die Einhaltung von rechtlichen Rahmenbedingungen.



4.1

Biometrische Daten sind Personendaten

Personendaten sind Angaben, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen (Art. 3 Bst. a DSGVO).

Biometrische Merkmale sind - wie bereits angeführt - in der Regel untrennbar mit einer bestimmten Person verknüpft. Daraus erstellte Rohdaten und Templates sind deshalb auch ohne weiteren Personenbezug (z.B. Name) Personendaten. Üblicherweise werden sie mit zusätzlichen Identifizierungs- resp. Adressierungsinformationen wie Name, Vorname, Geschlecht, Geburtsdatum usw. verknüpft. Die aus biometrischen Merkmalen erzeugten Rohdaten und Templates sind unter bestimmten Voraussetzungen **besonders schützenswerte Personendaten** (Art. 3 Bst. c Ziff. 2 DSGVO):

- Auf Grund ihrer Verwendung, namentlich in den Bereichen Gesundheit und Intimsphäre, Soziale Hilfe / Sozialversicherungen, Strafverfahren, administrative Verfahren, z.B. Foto in Krankengeschichte, DNA-Profil, das als erkennungsdienstliche Massnahme im Strafverfahren erhoben wird, oder
- wenn sie zur Erstellung von Persönlichkeitsprofilen dienen. Ein Persönlichkeitsprofil ist eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit der natürlichen Person erlaubt (Art. 3 Bst. d DSGVO), oder
- wenn aus ihnen allein, soweit technisch möglich, eindeutige Rückschlüsse auf körperliche oder charakterliche Eigenschaften oder die Gesundheit einer Person oder auch ihre ethnische Herkunft gemacht werden können. Zum Beispiel sind aus den biometrischen Rohdaten der Netzhaut (Retina) Diagnosen für Krankheiten wie Arteriosklerose oder Diabetes möglich. Der klassische Fingerabdruck lässt dagegen keine Aussagen über Erbanlagen oder Rückschlüsse auf Krankheiten zu (BGE 128 II 269 E. 3.3). Aus der Gangart einer Person kann möglicherweise geschlossen werden, dass sie an Parkinson leidet.

Biometrische Daten (Rohdaten oder Templates) sind also nicht per se besonders schützenswert im Sinne des Datenschutzrechts. Der Katalog der besonders schützenswerten Personendaten ist im DSGVO abschliessend. Ein offener Katalog lässt sich auch nicht aus der Bundesverfassung oder aus dem internationalen Recht ableiten.

4.2

Verfassungsrechtliche Rahmenbedingungen

4.2.1

Betroffene Grundrechte

Art. 7 BV bestimmt: «Die Würde des Menschen ist zu achten und zu schützen»

Als Achtungsgebot verbietet die Menschenwürde dem Staat, den Persönlichkeitswert des Menschen zu verletzen. Als Schutzpflicht gebietet sie ihm, Übergriffe Dritter in die Persönlichkeit des Einzelnen abzuwehren.

Kernaussage der Menschenwürde ist, dass ein Mensch nie als Objekt, sondern immer als Subjekt zu behandeln ist. Er darf nicht zu einem blossen Mittel, zu einer vertretbaren Grösse herabgewürdigt werden. Die Menschenwürde ist ein universelles Menschenrecht, das jedem Menschen kraft seiner Existenz voraussetzungslos gegenüber dem Staat und der Rechtsgemeinschaft zusteht.

Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten (Art. 13 Abs. 2 BV). Das Recht auf informationelle Selbstbestimmung gewährleistet die Befugnisse des Einzelnen, grundsätzlich selbst über die Preisgabe seiner Daten zu bestimmen.

Kann eine Person infolge fehlendem Merkmal oder Schwierigkeiten im Umgang mit dem System nicht eingelernt werden und demzufolge das biometrische Verfahren für sie nicht eingesetzt werden, müssen Alternativen zur Verfügung gestellt werden. Andernfalls ist das Diskriminierungsverbot und die Rechtsgleichheit (Art. 8 Abs. 1 und 2 BV) betroffen.

Die Rechte auf persönliche Freiheit und auf Achtung des Privat- und Familienlebens werden auch in völkerrechtlichen Verträgen garantiert (Art. 5 und 8 EMRK, SR 0.101, Art. 9 und 17 des Internationalen Paktes über bürgerliche und politische Rechte, UNO-Pakt II, SR 0.103.2).

4.2.2

Einschränkung der Grundrechte

Art. 36 BV legt zu Einschränkungen von Grundrechten fest:

- «1 Einschränkungen von Grundrechten bedürfen einer gesetzlichen Grundlage. Schwerwiegende Einschränkungen müssen im Gesetz selbst vorgesehen sein.
Ausgenommen sind Fälle ernster, unmittelbarer und nicht anders abwendbarer Gefahr.
- 2 Einschränkungen von Grundrechten müssen durch ein öffentliches Interesse oder durch den Schutz von Grundrechten Dritter gerechtfertigt sein.
- 3 Einschränkungen von Grundrechten müssen verhältnismässig sein.
- 4 Der Kerngehalt der Grundrechte ist unantastbar»

Die Menschenwürde darf nicht eingeschränkt werden, da ihr Geltungsbereich in der Regel mit ihrem Kerngehalt zusammenfällt.

Das Bundesgericht hat in BGE 128 II 269 f. E. 3.3 die Erstellung eines DNA-Profiles im Strafverfahren mittels Wangenschleimhautabstrich sowie dessen Bearbeitung im DNA-Informationssystem als leichte Eingriffe in die Rechte auf körperliche Integrität und auf informationelle Selbstbestimmung eingestuft. Ebenfalls als leichten Eingriff in die persönliche Freiheit erachtete das Bundesgericht die Erstellung und Aufbewahrung von erkennungsdienstlichem Material wie z.B. Fotografien (BGE 120 Ia 150 E. 2b). Der Kerngehalt des Grundrechts sei in diesen Beispielen nicht angetastet.

4.2.3

Verletzung der Menschenwürde

Die Menschenwürde wird immer dann verletzt, wenn biometrische Verfahren - auch in Kombination mit anderen technischen Anwendungen - dazu führen, dass der Mensch nur noch als Objekt, quasi wie eine Nummer, eine Ware, behandelt wird.

Beispiele eines menschenunwürdigen Einsatzes von Biometrie:

- Biometrische Rohdaten oder Templates werden flächendeckend in verschiedenen privaten und/oder staatlichen Lebensbereichen als Personenidentifikator eingesetzt, das heisst, unzählig viele Verknüpfungen mit Daten aus verschiedenen Datenbanken und die Erstellung von Persönlichkeitsprofilen sind möglich;
- Biometrische Rohdaten oder Templates aller Einwohnerinnen und Einwohner der Schweiz werden ohne bestimmte Zwecke in einer zentralen Datenbank auf unbestimmte Zeit (keine Aufbewahrungsdauer) gespeichert und einem unbestimmten Personenkreis aus Behörden und/oder Privaten zur Verfügung gestellt, z.B.

eine entsprechende DNA-Datenbank aller Einwohnerinnen und Einwohner, welche ausschliesslich zum Zweck hat, Behörden und Privaten (Versicherungen, Banken, usw.), den Abgleich mit eigenen personenbezogenen Daten inklusive allfälligen biometrischen Daten zu ermöglichen.

4.2.4

Verletzung des individuellen Selbstbestimmungsrechts

Das individuelle Selbstbestimmungsrecht wird immer dann verletzt, wenn biometrische Verfahren – auch in Kombination mit anderen technischen Anwendungen – die nachfolgend erläuterten datenschutzrechtlichen Rahmenbedingungen nicht erfüllen.

4.3

Datenschutzrechtliche Rahmenbedingungen

4.3.1

Einhaltung der allgemeinen datenschutzrechtlichen Grundsätze

Bei der Bearbeitung von biometrischen Daten sind die allgemeinen datenschutzrechtlichen Grundsätze einzuhalten. Diese werden nachfolgend erläutert.

4.3.2

Rechtsgrundlage

Gesetzliche Grundlage: Staatliche Organe dürfen biometrische Daten nur bearbeiten, wenn dies in einem Gesetz im formellen Sinn oder in einer Verordnung vorgesehen ist (Art. 17 Abs. 1 DSG). Werden biometrische Daten als besonders schützenswerte Personendaten bearbeitet, ist ein Gesetz im formellen Sinn erforderlich (Art. 17 Abs. 2 DSG).

Das gesetzliche Bestimmtheitsgebot ist gerade bei der Regelung biometrischer Daten strikte einzuhalten: Der Erlass muss ausdrücklich vorschreiben, wer (Datenherrin) was (welche biometrischen Merkmale) für welche klar bestimmten Zwecke (z.B. Identifizierung resp. Verifizierung von Personen) wie lange (Aufbewahrung, Vernichtung der biometrischen Daten) bearbeiten darf und wem (Aufzählung der Behörden) diese biometrischen Daten allfällig zu diesen Zwecken bekanntgegeben werden dürfen. Bei besonders schützenswerten Personendaten müssen diese Punkte im formellen Gesetz selbst vorgeschrieben werden. Details können aber auf Stufe Verordnung geregelt werden.

Einwilligung: Eine fehlende gesetzliche Grundlage kann unter Umständen im Einzelfall durch die Einwilligung der betroffenen Person ersetzt werden. Die betroffene Person muss vorgängig über die wesentlichen Punkte informiert werden: Verantwortliches staatliches Organ, die biometrischen Merkmale, Art und Zweck der Bearbeitung wie auch die Vernichtung der Daten. Nur so kann die betroffene Person einen freien Entscheid im Bewusstsein der möglichen Konsequenzen treffen. Bei besonders schützenswerten biometrischen Daten muss die Einwilligung ausdrücklich erfolgen (Art. 17 Abs. 2 Bst. c DSG).

4.3.3

Zweckbindung

Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Erhebung oder Beschaffung angegeben wurde, aus den Umständen ersichtlich oder in einem Gesetz oder in einer Verordnung vorgesehen ist (Art. 4 Abs. 3 DSG). Die technische Lösung ist so auszugestalten, dass der Zweck der Datenbearbeitung erreicht wird, Änderungen des Bearbeitungszweckes aber ausgeschlossen werden.

Die vier Bearbeitungsvorgänge – Erfassung Rohdaten und Erstellung Template, Speicherung Template, Erfassung Rohdaten und Erstellung Prüfmuster, Vergleich – haben möglichst in der Sphäre des Benutzers (betroffene Person) und nicht der Sphäre des Betreibers (verantwortliches Organ) zu erfolgen. Die betroffene Person kann so am besten kontrollieren, ob ihre biometrischen Daten zweckgebunden bearbeitet werden.

Durch technische Vorkehrungen ist auszuschliessen, dass aus Rohdaten oder Templates Zusatzinformationen wie klare Rückschlüsse auf Charaktereigenschaften oder eindeutige medizinische Diagnosen möglich sind. Zudem ist technisch sicherzustellen, dass eine zweckwidrige Verwendung von Randdaten (z.B. Logfiles) ausgeschlossen ist.

4.3.4

Verhältnismässigkeit

Wer Personendaten bearbeitet, hat die Verhältnismässigkeit zu beachten: Das Bearbeiten der Personendaten muss für die Erfüllung der Aufgaben geeignet und erforderlich sein (Art. 4 Abs. 2 DSGVO). Den Grundsätzen der Datenvermeidung und Datensparsamkeit ist Beachtung zu schenken. Sobald und soweit es möglich ist, sind Personendaten zudem zu anonymisieren oder zu pseudonymisieren.

Es ist abzuwägen, ob die Verwendung biometrischer Daten (Foto, Fingerprint-Template) gegenüber anderen Lösungen verhältnismässig erscheint. Dabei ist zu beachten, dass jede Bearbeitung von Personendaten einen Eingriff in das informationelle Selbstbestimmungsrecht darstellt und deshalb einer besonderen Begründung bedarf; Bequemlichkeit oder allgemeine Kundenfreundlichkeit genügen dafür grundsätzlich nicht. Soweit keine Alternativlösung besteht, ist ein biometrisches Verfahren mit Datenherrschaft bei der betroffenen Person zu bevorzugen (z.B. Smart-Card). Es ist zu prüfen und sicherzustellen, dass nur von geeigneten biometrischen Merkmalen der betroffenen Person (nahezu 100%ige Wahrscheinlichkeit) Rohdaten erstellt und daraus Templates erzeugt werden. Unter mehreren biometrischen Merkmalen sind diejenigen auszuwählen, welche am sichersten sind, also am nächsten diese 100%ige Wahrscheinlichkeit erreichen. Soweit der Einsatz biometrischer Merkmale geeignet und notwendig ist, sind möglichst einzig Templates, nicht aber Rohdaten zu speichern. Die betroffene Person sollte zudem selbst und freiwillig entscheiden können, ob und wem sie gespeicherte biometrische Daten weitergeben möchte.

Wird hingegen eine Bearbeitung und Speicherung biometrischer Daten in dezentralen und zentralen Datenbanken in der Herrschaft des Betreibers ins Auge gefasst, ist der Persönlichkeitsschutz der Nutzerinnen und Nutzer adäquat sicherzustellen. Der Zugriff auf diese biometrischen Daten ist auf einen möglichst kleinen Personenkreis zu beschränken.

Besondere Beachtung ist der Bearbeitung personenbezogener Randdaten zu schenken. Diese dürfen nicht personenbezogen abgelegt werden. Damit wird die Erstellung von Persönlichkeits- oder Bewegungsprofilen zumindest nicht erleichtert. Nicht mehr benötigte biometrische Daten sind in der Regel zu vernichten (Art. 21 DSGVO). Bei einer zentralen oder dezentralen Speicherung biometrischer Daten ist eine Aufbewahrungsdauer festzulegen.

4.3.5

Transparenz

Personendaten müssen in der Regel bei der betroffenen Person erhoben werden. Ausnahmen bedürfen einer Rechtsgrundlage (Art. 4 Abs. 2 und 18 DSGVO). Die betroffenen Personen müssen also über die Möglichkeit und Zulässigkeit der Bearbeitung ihrer biometrischen Daten klar informiert werden. Dies kann z.B. durch Informationsblätter, Informationen im Internet oder klaren Hinweistafeln erfolgen: Bei der Erhebung müssen die Betroffenen direkt mitwirken. Das Auslesen und Übermitteln von Rohdaten oder Templates muss für die betroffene Person ebenfalls transparent sein. Der Einsatz von Funktechnologie (RFID) ist nur mit Wissen der betroffenen Person zulässig.

4.3.6

Richtigkeit

Biometrische Daten müssen richtig und soweit es der Zweck des Bearbeitens verlangt, aktuell und vollständig sein (Art. 5 DSGVO). Es dürfen nur biometrische Verfahren eingesetzt werden, welche eine nahezu 100%ige Wahrscheinlichkeit der Identifikation oder Verifikation der betroffenen Person erlauben. Herstellerangaben zu Erkennungsquote und Fehlerrate sind zu hinterfragen und regelmässig zu überprüfen. Die Anforderungen an Erkennungsquote und Fehlerrate sind durch den Zweck der biometrischen Identifikation oder Verifikation bestimmt. Die zusätzliche Verwendung einer Smart-Card oder eines Tokens (Besitz) sowie die Eingaben eines Passwortes (Wissen) wird häufig unumgänglich sein. Mehrere biometrische Merkmale können auch kombiniert eingesetzt werden, wenn dies verhältnismässig ist und die Richtigkeit dadurch erhöht wird.

4.3.7

Kontrollrechte der betroffenen Person

Die datenschutzrechtlichen Auskunfts- und Einsichtsrechte, Berichtigungsrechte und übrigen Rechte zur Unterlassung, Feststellung oder Beseitigung rechtswidriger Bearbeitung biometrischer Daten müssen gewährleistet sein (Art. 25 DSGVO). Dabei müssen die Betreiber von biometrischen Verfahren darauf achten, dass sie auch technisch in der Lage sind, die Kontrollrechte der betroffenen Personen zu berücksichtigen: Wie wird die Einsicht gewährt? Wie können falsche Personendaten berichtigt werden? Wie können Fehler der Maschine durch den Menschen überstimmt werden? usw.

4.3.8

Datensicherheit

Daten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden (Art. 7 DSGVO sowie Art. 8 ff. und 20 ff. der Verordnung zum DSGVO). Je mehr und je sensiblere Daten bearbeitet werden, desto höher sind die Anforderungen an die Datensicherheit. Dabei ist der Verschlüsselung der Daten und Datenströme eine besondere Beachtung zu schenken.

4.3.9

Verantwortung

Für den Datenschutz ist das Organ verantwortlich, das die Personendaten zur Erfüllung seiner Aufgaben bearbeitet oder bearbeiten lässt (Art. 16 DSGVO).

Die Verantwortlichkeit ist klar festzulegen. Externen Dienstleistern sind die datenschutzrechtlichen Anforderungen zu überbinden. Besondere Aufmerksamkeit ist der Wahrung des Amtsgeheimnisses sowie besonderer Geheimhaltungspflichten zu widmen.

Anwendungsbeispiele

In den Tabellen im Anhang 1 sind zahlreiche Anwendungsbeispiele erwähnt. Dem Biometrie-Markt werden immense Wachstumsraten vorausgesagt.

5.1

Anwendungen durch staatliche Organe in der Schweiz

Gesichtsbilder

- Pass, Identitätskarte, Führerausweis, Abonnemente des öffentlichen Verkehrs, Personalausweise usw. mit zentralen Datenbanken;
- Automatisierte Gesichtserkennung: FAREC Zürich-Kloten (Versuchsbetrieb);
- Entsprechend den Anforderungen der USA und den Regelungen der EU sollen auch in der Schweiz ab 2007 biometrische Daten (Gesichtsbild, ev. Fingerabdruck oder Iris) in den Pass aufgenommen werden (siehe dazu: Fedpol, Erläuternder Bericht zum Vorentwurf zur Revision des Gesetzes und der Verordnung über Ausweise für Schweizer Staatsangehörige, S. 14, www.bap.admin.ch/d/themen/ausweise/biometrie/050621/Berichtd.pdf).

Fingerabdruck

- AFIS (Verordnung über die Bearbeitung erkennungsdienstlicher Daten, SR 361.3) schweizweit zentrale Datenbank, AFIS erlaubt Rückgriff auf Rohdaten;
- Strafuntersuchungen (kantonale Strafprozessordnungen);
- Fingerabdruck: Inhaber von Abonnenten eines kommunalen Schwimmbades.

DNA

- Strafuntersuchungen (DNA-Profilgesetz, SR 363), schweizweit zentrale Datenbank;
- Im DNA-Profil-Gesetz ist die Vernichtung der Probe nach der Analyse vorgesehen (Art. 9). Es darf weder nach dem Gesundheitszustand noch – mit Ausnahme des Geschlechtes – nach anderen persönlichen Eigenschaften geforscht werden. Das Analysematerial und das erstellte DNA-Profil dürfen nur für die im Gesetz vorgesehenen Zwecke verwendet werden (Art. 2 Abs. 2 DNA-Profil-Gesetz).

5.2

Anwendungen durch staatliche Organe in der EU

- Bild und Fingerabdruck in Visa und Aufenthaltsbewilligungen, europaweit zentrale Datenbank;
- Bild ab 2006 und Fingerabdruck ab 2008 in Pässen der EU.

5.3

Anwendungen durch staatliche Organe im übrigen Ausland

USA: Pass mit biometrischen Daten (Bild und Fingerabdruck) oder Visum / Erstellung Bild und Fingerabdruck bei Einreise;

Arabische Emirate (U.A.E.): Ausweise mit biometrischen Daten inklusive RFID;

Neuseeland: Zentrale Bilddatenbank aller Staatsangehörigen;

China / Macao: Projekt bei welchem 550'000 Bürger die Macao Multifunktion Smart ID Card mit biometrischen Merkmalen und digitaler Signatur erhalten haben (ID-Karte, Führerausweis, Studentenausweis, Medical Card, elektronische Geldbörse). Eine Vielzahl weiterer Beispiele in den verschiedenen Ländern befindet sich in HORNUNG GERRIT, Die digitale Identität, Rechtsprobleme von Chipkartenausweisen: Digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren, Diss. Kassel 2005, S. 81 ff. sowie S. 98 ff.

6

Datenschutzrechtliche Forderungen

- a** Der Einsatz biometrischer Verfahren darf nur im Rahmen verfassungsmässiger Grundsätze erfolgen. Insbesondere muss die Menschenwürde berücksichtigt werden, indem der Mensch nicht zum Objekt herabgewürdigt wird.
- b** Es dürfen nur technisch ausgereifte biometrische Verfahren verwendet werden, deren Trefferquote sich möglichst einer 100%iger Wahrscheinlichkeit annähern. Es sind technische Sicherheitsmassnahmen zu treffen, welche die Fehlerraten und negative Folgen von technischen Mängeln reduzieren (menschliches „over-ruling“).
- c** Die Datensicherheit muss bestmöglich gewährleistet werden. Insbesondere die Verschlüsselung muss bei Datenbanken bzw. bei der Übermittlung von Daten ernsthaft geprüft werden.
- d** Biometrische Daten gehören in den Herrschaftsbereich der betroffenen Person und nicht des Systembetreibers.
- e** Die Erfassung biometrischer Daten ist an enge Zweckbindungsregeln zu knüpfen; es ist auch auf technischer Ebene sicherzustellen, dass diese eingehalten werden.
- f** Die aus dem Grundsatz der Verhältnismässigkeit fliessenden Anforderungen (möglichst wenig, unsensible und dezentral gespeicherte Personendaten; Anonymisierung oder Pseudonymisierung; Vernichtung) sind bei der Bearbeitung biometrischer Daten wie auch von Randdaten biometrischer Systeme zu beachten.
- g** Der bessere gesetzliche Schutz biometrischer Daten (Haftungsrecht, Strafrecht) ist durch die zuständigen Parlamente zu prüfen.

Anhang1 Übersicht über biometrische Merkmale und Verfahren

Tabelle 1: Physiologische (passive) Merkmale: Statistische biometrische Verfahren und Bewertung

Merkmal	Details	Genauigkeit Einwilligung	Wissen	Praxistauglichkeit / Anwendungen	Bemerkungen
Fingerabdruck (Datkyloskopie)	Auswertung der Minutien (Verzweigungs- und Endpunkte der Hauttrillen)	Ja	beachtliche Unterschiede in Fehlerraten von verschiedenen Geräten; für sicherheitskritische Massenanwendung ungeeignet	■ praxiserprobt (Kriminalistik, AFIS, Eurodac, IAFIS des FBI, Benutzeridentifikation an Computern, Autos usw., Zutrittskontrolle) ■ sehr gutes Kosten-/Nutzenverhältnis für einfache Anwendungen mit geringeren Sicherheitsanforderungen ■ auch für Privatanwender grosse Angebotspalette (USB-Sticks, Laptops, Maus mit eingebautem Scanner; Software)	■ Scannertechnologien (Optisch: Ladungsunterschiede Hautoberfläche, Thermisch: Infrarot, Ultraschall) ■ Bedenken betr. Hygiene ■ Für rund 2 % der Bevölkerung ungeeignet ■ Fingerabdruckfälschung und Überlistung möglich ■ "Unverwechselbarkeit" umstritten (Alter, Verletzungen usw.)
Gesicht	versch. geometr. Muster aus Gesicht einer Person, aber auch von Fotos oder Videobildern (Abstand Augen zueinander, zu Nase, Kinn, Backenknochen oder lokale Form des Auges, der Nase usw.)	Nein	relativ eindeutige Muster, jedoch derzeit nicht sehr genaues Verfahren (Mimik, Alterung, Schminke, Behaarung, Aufnahmebedingungen); 20-1700 Merkmale	■ FAREC Flughafen Zürich, Flughafen Amsterdam, Flughafen Sydney (SmartGate), Videoaufnahmen an öff. Plätzen in London und Birmingham ■ (rudimentärer) Bildvergleich ist Teil von marktüblichen Bildverwaltungsprogrammen ■ nach der zweidimensionalen wird auch an der dreidimensionalen Gesichtserkennung gearbeitet	■ Bedingt geeignet für Übergang von Kindern zu Erwachsenen
Iris	Struktur des farbigen Ringbereiches um die Pupille	Ja	sehr hoch 50-250 Merkmale kein Alterungsprozess	■ einsatzreif; gewisse Flugpassagiere London Heathrow, Amsterdam und Frankfurt	■ Mit geöffnetem Auge bis wenige Sekunden in Scanner zu blicken ■ rel. hohe Kosten ■ ungeeignet für Blinde ■ allfällige langfristige gesundheitliche Folgen ungeklärt
Netzhaut (Retina)	Laser tastet durch die Pupille die Netzhaut ab	Ja	noch genauer als Iris	■ einsatzreif	■ Für ein paar Sekunden Kopf und Auge sehr ruhig zu halten ■ Bedenken gewisser Personen betr. Hygiene (Kopf) ■ sehr hohe Kosten ■ allfällige langfristige gesundheitliche Folgen ungeklärt
Handgeometrie	Länge der Finger und andere charakteristische Grössen der Hand	Ja	Genauigkeit relativ gering	■ praxiserprobt (Zutritt einzelne Banken, Einreise USA, Flughafenpersonal San Francisco) ■ in 90er-Jahren populär, wird abgelöst	■ Bedenken gewisser Personen betr. Hygiene
Ohr		Ja	individuell, aber starker Alterungsprozess; weniger hohe Qualität des Merkmals	■ nicht einsatzreif	■ Bedenken gewisser Personen betr. Hygiene
Blutbahnen, u.a. Venenmuster auf Handrücken		Ja	individuell, aber starker Alterungsprozess; weniger hohe Qualität des Merkmals	■ nicht einsatzreif	■ Bedenken gewisser Personen betr. Hygiene

Haut	Ja	individuell, aber starker Altersprozess; weniger hohe Qualität des Merkmals	■ nicht einsatzreif	■ Bedenken gewisser Personen betr. Hygiene
Fingernägel	Ja	individuell, aber starker Altersprozess; weniger hohe Qualität des Merkmals	■ nicht einsatzreif	■ Bedenken gewisser Personen betr. Hygiene
Geruch	Ja	Sensoren nehmen Geruch an best. Körperstellen oder aus dem Mund auf und analysieren die chem. Zusammensetzung der Geruchsmoleküle	noch gering	■ geringe Akzeptanz
Wärmeabstrahlung	(Nein)	z.B. des Gesichtes	noch gering	■ geringe Akzeptanz

Tabelle 2: Physikalisches Merkmal: Statische biometrische Verfahren und Bewertung

Merkmal	Details	Genauigkeit Einwilligung	Wissen	Praxistauglichkeit / Anwendungen	Bemerkungen
DNA-Analyse	Übereinstimmung verschiedener Abschnitte der DNA	(Ja)	nahezu 100%	■ praxiserprobt, keine vollautomatische Durchführung, dauert Minuten bis Stunden	■ sehr hohe Kosten ■ Haar eines andern u.U. leicht zu beschaffen

Tabelle 3: Verhaltensbasierte (aktive, behaviorale) Merkmale: Dynamische biometrische Verfahren und Bewertung

Merkmal	Details	Genauigkeit Einwilligung	Wissen	Praxistauglichkeit / Anwendungen	Bemerkungen
Stimme Sprechverhalten	Spracherkennung; Sprache kann aufgenommen und/oder elektronisch bearbeitet worden sein	Nein	Theoretisch hohe Erkennungsrate	■ stark reduziert (Störgeräusche, technische Defizite, Verstellen der Stimme, Emotionen Alterung, Krankheit) ■ Für Identifikation zu grosse Daten ■ ungeeignet für Stumme ■ Stimmerkennungssoftware (Diktieren) für Privatanwender	■ ev. Lippenbewegung zusätzlich einzubeziehen ■ vorgegebener / freier Text
Schrift Unterschrift Schreibverhalten	Übereinstimmung zweier Bilder (Schriftproben) und/oder dynamische Auswertung von Stiftposition, Anpressdruck und Stiftwinkel	(Ja)	In Praxis meist auf Unterschrift beschränkt, deshalb Sicherheit sehr eingeschränkt	■ praxiserprobt bei Unterschriften	■ vorgegebener / freier Text
Dynamik Tastenanschlag Schreibverhalten	Messung der Verzögerung zwei aufeinander folgender Tastendrücken, Tastendruckdauer, Positionierung der Finger und Anpressdruck.	Ja	relativ ungenau, hängt sehr von Tätigkeit und Verfassung der Person ab		■ vorgegebener / freier Text ■ Bei fest vorgegebenem Text Parameter relativ konstant ■ Bedenken gewisser Personen betr. Hygiene
Gang/Bewegung	Erkennung des Ganges (Schrittfolge, Schrittlänge, Bewegungsablauf) oder anderer charakteristischer Bewegungseigenschaften	Nein	genauer als angenommen, sofern genügend Parameter, jedoch viele Einflussfaktoren (Schuhe, Kleidung, Schwangerschaft, Alkoholkonsum)	■ in Einzelfällen erprobt	

Anhang 2

Checkliste zur datenschutzrechtlichen Beurteilung biometrischer Projekte im öffentlich-rechtlichen Bereich

Begriffe

Was ist ein biometrisches Merkmal?	Biometrische Merkmale sind spezielle körpereigene Kennzeichen einer Person, die – zumindest theoretisch – immer und überall eindeutig mit nahezu 100%iger Sicherheit nur dieser einen Person zugeordnet werden können. Biometrische Merkmale lassen sich derzeit nur ausnahmsweise und mit erheblichem Aufwand verändern. Aus ihnen gewonnene biometrische Daten sind deshalb nicht nur personenbezogen, sondern personengebunden.
Was ist ein biometrisches Verfahren?	Biometrische Verfahren beruhen auf physiologischen, verhaltenstypischen oder physikalischen Charakteristika von Menschen (biometrischen Merkmalen); durch eine geeignete Auswahl dieser Charakteristika lässt sich eine eindeutige Zuordnung zu einem bestimmten Menschen erreichen. Ein biometrisches Verfahren läuft wie folgt ab: ■ Erfassung des Merkmals mit einem Sensor (z.B. Kamera, Mikrofon, Tastatur, Spezialsensor zur Aufnahme von Gerüchen oder Fingerabdruck); Entnahme eines elektronischen Abdrucks (biometrische Rohdaten wie Foto, Sprachaufnahme, Videoaufnahme); ■ Im biometrischen Verfahren wird ein spezielles Mustergenerierungs- oder Mustereerkennungsverfahren (Algorithmus) eingesetzt und aus dem Merkmal ein Muster (Template) des Abdrucks des personengebundenen Merkmals generiert (Feature Extraction); das erzeugte Template wird abgelegt. ■ Ein auf dieselbe Weise erzeugtes Prüfmuster wird auf Übereinstimmung mit dem abgelegten Template oder einer Vielzahl von Mustern geprüft (Template Matching).
Was bedeuten Identifikation und Verifikation?	Verifikation: 1:1-Vergleich (one-to-one matching): die Eingangsdaten werden mit Referenzdaten der Person verglichen, als die sich der Nutzer ausgibt, um deren Identität zu bestätigen. Ziel ist die Bestätigung resp. Nichtbestätigung der geltend gemachten Identität. Identifikation: 1:n-Vergleich (one-to-many matching) mit den gespeicherten Referenzdaten vieler Individuen. Ziel ist die Feststellung der Identität einer Person; Personen werden aus einer Masse von anderen Personen erkannt.
Was ist der Unterschied zwischen Identifikation und Feststellung der Identität einer Person?	Die technischen Begriffe Verifikation und Identifikation beschreiben die Art des Vergleiches von Template und Prüfmuster. Die Identität einer Person wird seit Jahrhunderten und bis heute über ihren Namen, ihr Geschlecht, ihr Geburtsdatum und Heimort/Staatsangehörigkeit sowie ihren Familienbezug (Name und Geburtsdaten der Eltern) definiert. Dementsprechend erfolgt der Beweis der Identität einer Person vorab mittels Dokumenten (Pass, Geburtsurkunde, Familienbuch) und Registereinträgen (Geburtsregister, Familienregister, Einwohnerkontrolle). Biometrische Verfahren erlauben die Identifizierung einer Person auf technischem Weg; die Zuordnung von Rohdaten oder einem Template (sofern Algorithmus bekannt) zu einer Person genügt grundsätzlich zur Feststellung ihrer Identität.
Was ist ein Personenidentifikator?	In vielen Bereichen wird einer Person zusätzlich oder anstelle ihrer Angaben zur Identität ein eindeutiger, jedoch veränderbarer Personenidentifikator (in Deutschland: Personenkennziffer PKZ) zugeordnet (Kundenummer, AHV-Nummer). Es ist möglich, ein Template als solchen Identifikatoren zu verwenden. Dieser ist – sofern mit demselben Algorithmus erzeugt – nicht veränderbar. Für biometrische Daten gelten deshalb dieselben verfassungs- und datenschutzrechtlichen Anforderungen wie für andere Personenidentifikatoren.

Rechtmässigkeit

Werden Personendaten bearbeitet?	Personendaten sind Angaben, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen (Art. 3 Bst. a DSGVO). Aufgrund der Einmaligkeit der biometrischen Merkmale sind Templates und Rohdaten auch ohne weiteren Personenbezug (z.B. Name) Personendaten, oft sogar besonders schützenswerte.
Unter welcher Voraussetzung dürfen Personendaten durch staatliche Organe bearbeitet werden?	Staatliche Organe dürfen biometrische Daten nur bearbeiten, wenn dies in einem Gesetz im formellen Sinn oder in einer Verordnung vorgesehen ist (Art. 17 Abs. 1 DSGVO). Das gesetzliche Bestimmtheitsgebot ist gerade bei der Regelung biometrischer Daten strikte einzuhalten: Der Erlass muss ausdrücklich vorschreiben, wer (Datenherrin) was (welche biometrischen Merkmale) für welche klar bestimmten Zwecke (z.B. Identifizierung resp. Verifizierung von Personen) wie lange (Aufbewahrung, Vernichtung der biometrischen Daten) bearbeiten darf und wem (Aufzählung der Behörden) diese biometrischen Daten allfällig zu diesen Zwecken bekannt gegeben werden dürfen.

Werden besonders schützenswerte Personendaten bearbeitet?

Die aus biometrischen Merkmalen erzeugten Rohdaten und Templates sind unter bestimmten Voraussetzungen besonders schützenswerte Personendaten (Art. 3 Bst. c Ziff. 2 DSG), nämlich

- wenn sie in einem im Datenschutzgesetz definierten Bereich (Gesundheitsbereich, Sozialbereich oder Strafrechtsbereich) verwendet werden oder
- wenn sie zur Erstellung von Persönlichkeitsprofilen dienen. Ein Persönlichkeitsprofil ist eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit der natürlichen Person erlaubt (Art. 3 Bst. d DSG), oder
- wenn das zur Anwendung gelangende Datenschutzgesetz die besonders schützenswerten Personendaten nicht abschliessend aufzählt.

Aus physikalischen Merkmalen (DNA) gewonnene Rohdaten zählen aufgrund der mit ihrer Verwendung verbundenen besonderen Gefahr einer Persönlichkeitsverletzung zu den besonders schützenswerten Personendaten. Dasselbe gilt für physiologische und verhaltensbasierte Merkmale, soweit die Technik es erlaubt, mittels derselben eindeutige Rückschlüsse auf Krankheiten oder bestimmte Charaktereigenschaften einer Person zu schliessen.

Werden biometrische Daten als besonders schützenswerte Personendaten bearbeitet, ist ein Gesetz im formellen Sinn erforderlich (Art. 17 Abs. 2 DSG).

Bei besonders schützenswerten Personendaten müssen die bearbeiteten biometrischen Merkmale, die Art und der Zweck der Verarbeitung wie auch die Vernichtung der Daten in einem formellen Gesetz selbst vorgeschrieben werden. Details können aber auf Stufe Verordnung geregelt werden.

Kann eine Einwilligung eine fehlende gesetzliche Grundlage für die Bearbeitung besonders schützenswerter Personendaten ersetzen?

Eine fehlende gesetzliche Grundlage kann im Einzelfall durch die Einwilligung der betroffenen Person ersetzt werden. Die betroffene Person muss vorgängig über die wesentlichen Punkte informiert werden: Verantwortliches staatliches Organ, die biometrischen Merkmale, Art und Zweck der Bearbeitung wie auch die Vernichtung der Daten. Es besteht eine freie Wahlmöglichkeit ohne Nachteile für den Fall des Verzichts (u.a. Preisunterschied, zusätzliche Wartezeit). Nur so kann die betroffene Person einen freien Entscheid im Bewusstsein der möglichen Konsequenzen treffen. Bei besonders schützenswerten biometrischen Daten muss die Einwilligung ausdrücklich erfolgen (Art. 17 Abs. 2 Bst. c DSG).

Gibt es verfassungsrechtliche Schranken?

Die Würde des Menschen ist zu achten und zu schützen (Art. 7 BV); der Mensch darf durch biometrische Verfahren nicht zum Objekt herabgewürdigt werden. Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten (Art. 13 Abs. 2 BV).

Zu Einschränkungen von Grundrechten legt Art. 36 BV fest:

- Einschränkungen von Grundrechten bedürfen einer gesetzlichen Grundlage. Schwerwiegende Einschränkungen müssen im Gesetz selbst vorgesehen sein. Ausgenommen sind Fälle erster, unmittelbarer und nicht anders abwendbarer Gefahr.
- Einschränkungen von Grundrechten müssen durch ein öffentliches Interesse oder durch den Schutz von Grundrechten Dritter gerechtfertigt sein.
- Der Kerngehalt der Grundrechte ist unantastbar.

Ist ein Eingriff in die körperliche Integrität zulässig?

Es kann nicht ausgeschlossen werden, dass das Erfassen gewisser biometrischer Daten gesundheitliche Störungen verursachen kann (z.B. Iris-Scan).

Ein Eingriff in die körperliche Integrität bedarf einer besonderen formell-gesetzlichen Grundlage. Solange gesundheitliche Nebenwirkungen beim Einsatz eines biometrischen Verfahrens nicht ausgeschlossen werden können, darf dieses nur mit entsprechender gesetzlicher Ermächtigung eingesetzt werden.

Zweckbindung

Werden Personendaten bearbeitet?

Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Erhebung oder Beschaffung angegeben wurde, aus den Umständen ersichtlich oder in einem Gesetz oder in einer Verordnung vorgesehen ist (Art. 4 Abs. 3 DSG).

Eine Änderung des ursprünglichen Bearbeitungszweckes kann durch die betroffene Person kaum kontrolliert werden. Die technische Lösung ist deshalb so auszugestalten, dass der Zweck der Datenbearbeitung erreicht wird, eine Änderung des Bearbeitungszweckes aber möglichst ausgeschlossen wird.

Welche Bearbeitungsvorgänge finden in der Betreibersphäre, welche in der Nutzersphäre statt?

Alle Vorgänge eines biometrischen Verfahrens haben möglichst in der Nutzer- und nicht der Betreibersphäre stattzufinden. Es genügt deshalb in der Regel nicht nur das Template der betroffenen Person auf einer Smartcard ("Chipkarte") oder einem USB-Token zu speichern. Ist eine Verifikation der Zweck des Einsatzes biometrischer Daten, ist die Ablage von Templates und Rohdaten in einer Datenbank grundsätzlich nicht statthaft; Ausnahmen bedürfen einer besonderen Begründung.

On-Card-Matching-Technologie erlaubt es, dass auf der Karte zusätzlich auch der Vergleich mit dem Template stattfindet. Findet die Erstellung von Template und Prüfmuster in der Betreibersphäre statt, ist sicherzustellen, dass Rohdaten und Template nicht zweckfremd verwendet werden können.

Mittels eines in einen USB-Token eingebauten Fingerprint-Scanners können auch die Erfassungsvorgänge benutzerseitig ausgeführt werden. Ein solcher Token enthält ein komplettes System zur biometrischen Authentisierung; biometrische Daten werden ausserhalb des Tokens keine verarbeitet oder abgelegt.

Werden Rohdaten bearbeitet?

Nur aus Rohdaten lässt sich ein Template erzeugen. Rohdaten dürfen jedoch nur zur Erstellung von Templates und Prüfmustern verwendet werden. Die Ablage von Rohdaten ausserhalb des flüchtigen Zwischenspeichers einer geschlossenen Einheit während des Erzeugungsvorganges bedarf einer besonderen Begründung.

Lassen sich aus den Rohdaten Zusatzinformationen entnehmen?

Es ist sicherzustellen, dass aus Rohdaten und Templates keine Nebenerkenntnisse (Hinweise auf Krankheiten, Charaktereigenschaften usw.) gewonnen werden. Solche Nebenerkenntnisse können unter die besonders schützenswerten Personendaten fallen; die Gewinnung von Nebenerkenntnissen ist eine unzulässige Änderung des Bearbeitungszweckes.

Lassen sich aus den Randdaten Zusatzinformationen entnehmen?	Biometrische Verfahren erleichtern die Gewinnung von Informationen über das Verhalten der betroffenen Personen. Es ist sicherzustellen, dass eine zweckwidrige Verwendung von Randdaten (Logfiles usw.) ausgeschlossen ist.
Wird bei der Erzeugung von Templates ein Standard-Algorithmus verwendet?	Wird ein Standardalgorithmus verwendet, besteht die Gefahr von zweckwidrigen Template-Vergleichen und der Erstellung von Persönlichkeitsprofilen mittels Verknüpfung über das Template. Es ist deshalb darauf zu achten, dass ein Template möglichst nicht mit einem Standardalgorithmus erzeugt wird. Es ist sicherzustellen, dass der Algorithmus keine Wiederherstellung der Rohdaten zulässt.

Verhältnismässigkeit

Wer Personendaten bearbeitet, hat die Verhältnismässigkeit zu beobachten: Das Bearbeiten der Personendaten muss für die Erfüllung der Aufgaben geeignet und erforderlich sein (Art. 4 Abs. 2 DSGVO).	
Welche Kriterien hat die Verhältnismässigkeit zu erfüllen?	Datenbearbeitungssysteme und -programme sind so zu gestalten, dass so wenig, so unsensibel und so dezentral gespeicherte Personendaten wie möglich anfallen (Datenvermeidung und Datensparsamkeit). Sobald und soweit es möglich ist, sind Personendaten zu anonymisieren oder zu pseudonymisieren. Nicht mehr benötigte Daten sind zu vernichten. Ein entsprechendes Konzept ist zu erstellen. Bei jedem biometrischen Verfahren werden Personendaten bearbeitet; eine Anonymität ist nicht möglich; dies im Gegensatz zu Verfahren, welche auf dem Besitz (Schlüssel) oder Wissen (Passwort) beruhen. Wenn der gewünschte Effekt mit einem weniger grossen Eingriff in die Persönlichkeitsrechte erzielt werden kann, ist die Alternativ-Lösung zu wählen. Beispiel: ■ Eine Person möchte ein nicht übertragbares Jahresabonnement für den Museumseintritt lösen. Beim Museumseintritt ist eine Autorisierung vorzunehmen. Eine solche Prüfung kann mittels Passwort oder biometrischem Merkmal vorgenommen werden. Es ist nicht erforderlich, die Person namentlich zu kennen. ■ Beim Einsatz eines Passwortes ist es nicht nötig, personenbezogene Daten zu bearbeiten; die betroffene Person kann anonym eine übertragbare Jahreskarte lösen. Beim Einsatz eines biometrischen Verfahrens ist eine Anonymität nicht möglich. Anstelle einer Zuordnung weiterer Personendaten zu den biometrischen Daten kann ein Pseudonym verwendet werden (z.B. Hans Muster, Kunde1, Benutzer-ID). ■ Es ist abzuwägen, ob die Verwendung biometrischer Daten (Foto, Fingerprint-Template) gegenüber der Passwort-Lösung verhältnismässig erscheint. Dabei ist zu beachten, dass jede Bearbeitung von Personendaten einen Eingriff in das informationelle Selbstbestimmungsrecht darstellt und deshalb einer besonderen Begründung bedarf; Bequemlichkeit oder allgemeine Kundentreue genügen dafür grundsätzlich nicht. ■ Die biometrische Lösung im erwähnten Beispiel könnte darin bestehen, dass die Person gegen Barzahlung einen entsprechenden Ausweis mit Foto erhält. Anstelle des Fotos könnte auch ein Template des Fingerabdruckes verwendet werden. Zu beachten sind in beiden Fällen die übrigen Anforderungen an biometrische Verfahren. Nein. Für alle biometrischen Verfahren gelten dieselben Anforderungen.
Eine Identifikation oder Verifikation muss als solche dem Grundsatz der Verhältnismässigkeit entsprechen. Der gewünschte Effekt ist mit keinem oder einem möglichst kleinem Eingriff in die Persönlichkeitsrechte zu erzielen.	
Welche Informationen über das Verhalten der betroffenen Person werden aus der elektronischen Verifikation/Identifikation gewonnen?	Die elektronische Verifikation/Identifikation erleichtert die Gewinnung von Informationen über das Verhalten der betroffenen Person. Die Aufzeichnung und Auswertung von personenbezogenen Randdaten (Logging) muss den skizzierten Anforderungen an die Verhältnismässigkeit bei der Datenbearbeitung genügen (möglichst wenig, unsensibel und dezentral gespeicherte Personendaten; Anonymisierung oder Pseudonymisierung; Vernichtung). Ein entsprechendes Konzept ist zu erstellen.
Wie lange werden Personendaten aufbewahrt und was passiert mit ihnen nach Ablauf der Aufbewahrungsfrist?	Nicht mehr benötigte biometrische Daten sind zu vernichten, sofern sie nicht der Archivbehörde zuzustellen sind (Art. 21 DSGVO)
Welche Bearbeitungsvorgänge finden in der Betreibersphäre, welche in der Nutzersphäre statt?	Siehe unter „Zweckbindung“
Werden Rohdaten bearbeitet?	Siehe unter „Zweckbindung“

Integrität: Vollständigkeit und Richtigkeit

Ermöglichen biometrische Verfahren eine richtige Identifikation oder Verifikation?	Biometrische Daten müssen richtig und soweit es der Zweck des Bearbeitens verlangt, aktuell und vollständig sein (Art. 5 DSGVO). Die Sicherheit von biometrischen Verfahren hängt von Wahrscheinlichkeiten ab, die Verfahren müssen kalibriert werden. Eine 100%ige Sicherheit gibt es nicht. Zwei Templates stimmen bei derselben Person kaum oder nie 100%ig überein: Wärme, Kälte, Stimmungen, Alterung, Tätigkeiten usw. führen zu leichten Merkmalsveränderungen. Dazu kommen Messunterschiede. Viele Templates sind deshalb extrem ähnlich; beinah biometrische Zwillinge müssen jedoch als solche erkannt werden. Die Anforderungen an den Anteil der falsch zurückgewiesenen Nutzer (FRR, False Rejection Rate) sowie den Anteil der fälschlich vom System zugelassenen Personen (FAR, False Acceptance Rate) werden durch den Zweck der biometrischen Identifikation oder Verifikation bestimmt. Die tatsächliche Erkennungsquote und Fehlerrate sind regelmässig zu überprüfen; Herstellerangaben sind kritisch zu hinterfragen. Um die Überlistung des Erfassungsvorganges ("Gummifinger", Foto einer fremden Iris vor Auge) zu erschweren, ist es erforderlich, zu erkennen, ob das Merkmal Teil einer lebenden Person ist. Bei sicherheitskritischen Anwendungen wird die zusätzliche Verwendung einer Smartcard oder eines Tokens (Besitz) sowie die Eingabe eines Passwortes (Wissen) häufig unumgänglich sein. Mehrere biometrische Merkmale können auch kombiniert eingesetzt werden. Ein gewisser Prozentsatz von Personen kann auf einem System nicht eingelesen werden, weil sie nicht über das entsprechende biometrische Merkmal verfügen oder Schwierigkeiten bei der Erfassung des Merkmals haben (FER: Failure to enrol rate). Für diese Personen ist ein Alternativszenario, welches nicht zu einer Diskriminierung der betroffenen Person führen darf, vorzusehen. Beim Fingerabdruck wird von einer Rate von 2% ausgegangen, d.h. hochgerechnet rund 150'000 Personen in der Schweiz. Biometrische Verfahren werden durch Automatisierung (Maschinen) dominiert. Der menschliche Beitrag ist oft gering. Wenn es zu einem Fehler kommt, muss aber der Mensch die Maschine übersteuern können, um die Folgen eines Fehlers so gering wie möglich halten zu können („over-ruling“).
Was geschieht, wenn eine Person nicht (mehr) über das verwendete biometrische Merkmal verfügt?	
Was geschieht wenn eine Person zu Unrecht erkannt oder eben nicht erkannt wird?	

Sicherheit

Wie ist die Sicherheit der bearbeiteten Daten gewährleistet?	Daten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden (Art. 7 DSGVO). Je mehr und je sensiblere Daten bearbeitet werden, desto höher sind die Anforderungen an die Sicherheit. Der Schutz gegen unbefugtes Bearbeiten ist nach innen wie nach aussen zu gewährleisten (z.B. Verschlüsselung). Rohdaten und Templates dürfen nur in einer besonders gesicherten Umgebung bearbeitet werden. Die Verwendung von Standard-Datenformaten erleichtert die Verwendung der Daten zu einem anderen als dem ursprünglich vorgesehenen Zweck. Entsprechende Anforderungen sind betreffend Sicherheit der Daten zu ergreifen. Durch technische und organisatorische Massnahmen sind Manipulationen an Hard- und Software (USB Sniffer, Hacking) zu verhindern. Ein Datenschutz- und Sicherheitskonzept regelt auch Zugriffs- und Zutrittsrechte sowie die Entwicklung und Wartung des Systems. Dazu gehört auch ein Betriebsreglement.
--	--

Transparenz

Ist die Erhebung von Personendaten für die betroffene Person transparent?	Personendaten müssen in der Regel bei der betroffenen Person erhoben werden. Ausnahmen bedürfen einer Rechtsgrundlage (Art. 4 Abs. 2 und 18 DSGVO). Die Erhebung von Personendaten muss für die betroffene Person transparent sein. Gewisse biometrische Merkmale können ohne Wissen und Willen der betroffenen Person erfasst werden. Dies ist unzulässig.
Können Templates oder Rohdaten ohne Mitwirkung des Betroffenen übermittelt werden (RFID)?	Das Auslesen und Übermitteln von Personendaten muss für die betroffene Person transparent sein. Der Einsatz von Funktechnologie ist nur mit Wissen der betroffenen Person zulässig.

Verantwortung

Wer ist für die Datenbearbeitung und die Einhaltung der datenschutzrechtlichen Anforderungen verantwortlich?	Für den Datenschutz ist das Organ verantwortlich, das die Personendaten zur Erfüllung seiner Aufgaben bearbeitet oder bearbeitet lässt (Art. 16 DSGVO). Die Verantwortlichkeit ist klar festzulegen.
Bearbeiten externe Dienstleister Daten?	Externen Dienstleistern sind die datenschutzrechtlichen Anforderungen zu überbinden. Besondere Aufmerksamkeit ist der Wahrung des Amtsgeheimnisses sowie besonderer Geheimhaltungspflichten zu widmen.

Rechte der betroffenen Person

Welche Rechte haben betroffene Personen?	Die datenschutzrechtlichen Auskunfts- und Einsichtsrechte, Berichtigungsrechte und übrigen Rechte zur Unterlassung, Feststellung oder Beseitigung rechtswidriger Bearbeitung biometrischer Daten müssen gewährleistet sein (Art. 8, 15 und 25 DSGVO). Dies ist durch den Betreiber sicher zu stellen.
Wie ist der Umgang mit Fehlern?	Jedes biometrische Verfahren kann fehlerhafte Ergebnisse verursachen. Die zu Unrecht abgewiesene Person muss über eine Möglichkeit verfügen, ihr Recht durchzusetzen. Dafür bedarf es in der Regel eines Korrektursystems, welches dem Betreiber erlaubt, die automatischen Ergebnisse zu überstimmen (over-ruling).

Anhang 3 Literaturhinweise

Vorbemerkungen:

Die nachfolgenden Literaturhinweise erheben keinen Anspruch auf Vollständigkeit und widerspiegeln die Situation per 1. Dezember 2005 (insbesondere die Verweise auf Internetadressen). Es wurden vor allem deutschsprachige Werke berücksichtigt. Selbstverständlich ist aber bei einem solchen (globalen) Thema auch anderssprachige Literatur von Bedeutung.
Zusätzlich zu beachten ist das CISA-Newsletter Juni 2005 mit Schwerpunkt Biométrie.

Albrecht Astrid	Biometrie und Recht. in: Nolde Veronika/Leger Lothar (Hrsg.), Biometrische Verfahren, Körpermerkmale als Passwort: Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, S. 97 ff.
Dieselbe	Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, Diss. Frankfurt am Main 2003
Dieselbe	Biometrie zum Nutzen für Verbraucher?, Kriterien der Verbraucherfreundlichkeit biometrischer Verfahren, DuD 2000, S. 332 ff.
Dieselbe	Relevanz biometrischer Verfahren im gesellschaftlichen Kontext, in: Nolde Veronika/Leger Lothar (Hrsg.), Biometrische Verfahren, Körpermerkmale als Passwort: Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, S. 85 ff.
Dieselbe	Verbraucherpolitische Bedeutung der Biometrie, in: Nolde Veronika/Leger Lothar (Hrsg.), Biometrische Verfahren, Körpermerkmale als Passwort: Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, S. 129 ff.
Albrecht Astrid Probst Thomas	Bedeutung der politischen und rechtlichen Rahmenbedingungen für biometrische Identifikationssysteme, in: Behrens Michael/Roth Richard (Hrsg.), Biometrische Identifikation, Braunschweig/Wiesbaden 2001, S. 27 ff.
Artikel-29-Datenschutzgruppe	Stellungnahme Nr. 7/2004 vom 11. August 2004 zur Aufnahme biometrischer Merkmale in Visa und Aufenthaltstitel unter Berücksichtigung des Aufbaus des Visa-Informationssystemsystems VIS und Working document on biometrics vom 1. August 2003
Bäumler Helmut Gundermann Lukas Probst Thomas	Stand der nationalen und internationalen Diskussion zum Thema Datenschutz bei biometrischen Systemen, Datenschutz bei biometrischen Systemen, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel August 2001
Behrens Michael Heumann Björn	Fingerbildererkennung, in: Behrens Michael/Roth Richard (Hrsg.), Biometrische Identifikation, Braunschweig/Wiesbaden 2001, S. 81 ff.
Bleumer Gerrit	Biometrische Ausweise, Schutz von Personenidentitäten trotz biometrischer Erkennung, DuD 1999, S. 155 ff.
Borking John Verhaar Paul	Biometrie und Datenschutz, Bedrohungen und Privacy-Enhancing Technologies, DuD 1999, S. 138 ff.

Büllingen Franz Hillebrand Annette	Biometrie als Teil der Sicherungsinfrastruktur?, DuD 2000, S. 339 ff.
Dieselbe	Technikfolgenabschätzung und Akzeptanzforschung beim Einsatz biometrischer Verfahren, in: Nolde Veronika/Leger Lothar (Hrsg.), Biometrische Verfahren, Körpermerkmale als Passwort: Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, S. 420 ff.
Bundesamt für Sicherheit in der Informationstechnik	BioFace, Vergleichende Untersuchung von Gesichtserkennungssystemen, Version 2.1, Juni 2003
Busch Christoph Daum Henning	Frei von Zweifel? Biometrische Erkennung: Grundlagen, Verfahren, Sicherheit, c't 5/2002
Daugman John	Irserkennung, in: Behrens Michael/ Roth Richard (Hrsg.), Biometrische Identifikation, Braunschweig/ Wiesbaden 2001, S. 129 ff.
Donnerhacke Lutz	Anonyme Biometrie, DuD 1999, S. 151 ff.
Dornberger Rolf Probst Fabian	Biometrics, ein Überblick, Fachhochschule Solothurn Nordwestschweiz, 2003
Dürig Günther Maunz Theodor (Hrsg.)	Grundgesetz, Kommentierung der Artikel 1 und 2 Grundgesetz von Günter Dürig, Sonderauflage, München 2003
Ehrenzeller Bernhard Mastrorardi Philippe Schweizer Rainer J. Vallander Klaus (Hrsg.)	Die Schweizerische Bundesverfassung, Kommentar, Zürich/Basel/Genf/Lachen 2002
Europarat	Rapport sur l'application des principes de la convention 108 à la collecte et au traitement des données biométriques (T-PD, 2-4 février 2005) http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNIL-biometrie/T-PD 2005 BIOM F.pdf
Fedpol	Erläuternder Bericht zum Vorentwurf zur Revision des Gesetzes und der Verordnung über Ausweise für Schweizer Staatsangehörige, S. 14, http://www.bap.admin.ch/d/themen/ausweise/biometrie/050621_Bericht_d.pdf
Giesecke Hans-Joachim Kalo Horst Lassmann Gunter	Erfahrungen mit biometrischen Systemen, in: Nolde Veronika/Leger Lothar (Hrsg.), Biometrische Verfahren, Körpermerkmale als Passwort: Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, S. 378 ff.
Golembiewski Claudia Probst Thomas	Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel Juli 2003
Gundermann Lukas Köhntopp Marit	Biometrie zwischen Bond und Big Brother, Technische Möglichkeiten und rechtliche Grenzen, DuD 1999, S. 143 ff.
Gundermann Lukas Probst Thomas	Biometrie, in: Rossmagel Alexander (Hrsg.), Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003, S. 1967 ff.
Harb Beda Schmid Daniel	Der Einsatz biometrischer Systeme, digma 2005, S. 158 ff.
Hornung Gerrit	Der Personenbezug biometrischer Daten, Zugleich eine Erwiderung auf Saeltzer, DuD 2004, S. 218 ff., DuD 2004, S. 429 ff.
Derselbe	Die digitale Identität, Rechtsprobleme von Chipkartenausweisen: Digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren, Diss. Kassel 2005
Klische Marcus	Multimodale biometrische Authentisierung – Erhöhte Erkennungsgenauigkeit und Toleranz durch Kombination mehrerer Merkmale, in: Nolde Veronika/Leger Lothar (Hrsg.), Biometrische Verfahren, Körpermerkmale als Passwort: Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, S. 292 ff.
Köhntopp Marit	Multimodale biometrische Authentisierung – Erhöhte Erkennungsgenauigkeit und Toleranz durch Kombination mehrerer Merkmale, in: Nolde Veronika/Leger Lothar (Hrsg.), Biometrische Verfahren, Körpermerkmale als Passwort: Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, S. 292 ff.
Kuip Anton	Vergleich biometrischer Erkennungssysteme sowie deren Weiterentwicklung in der Praxis, in: Nolde Veronika/Leger Lothar (Hrsg.), Biometrische Verfahren, Körpermerkmale als Passwort: Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, S. 367 ff.
Lassmann Gunter	Bewertungskriterien zum Vergleich biometrischer Verfahren, Kriterienkatalog der Arbeitsgruppe 6 „Biometrische Identifikationsverfahren“ von TeleTrusTDeutschland e.V., DuD 1999, S. 135 ff.
Maurer Urs Vogt Nedim Peter (Hrsg.)	Kommentar zum schweizerischen Datenschutzgesetz, Basel/Frankfurt a.M. 1995

Müller Klaus Pfau Axel	Biometrische Verfahren zur Verifikation der Personen Identität, DuD 1992, S. 346 ff.
Nolde Veronika	Grundlegende Aspekte biometrischer Verfahren, in: Nolde Veronika/Leger Lothar (Hrsg.): Biometrische Verfahren, Körpermerkmale als Passwort: Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, S. 20 ff.
Pfitzmann Andreas	Biometrie – wie einsetzen und wie nicht, digma 2005, S. 154 ff.
Probst Thomas	Biometrie aus datenschutzrechtlicher Sicht, in: Nolde Veronika/Leger Lothar (Hrsg.), Biometrische Verfahren, Körpermerkmale als Passwort: Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, S. 115 ff.
Robra Uwe	Biometrie und Datenschutz, http://www.lfd.niedersachsen.de/master/C27956_N13146_L20_D0_I560.html
Rossnagel Alexander Hornung Gerrit	Biometrische Daten in Ausweisen, DuD 2005, S. 69 ff.
Saeltzer Gerhard	Sind diese Daten personenbezogen oder nicht?, Wie der Personenbezug von Daten, auch biometrischer, sich fundiert prüfen lässt , DuD 2004, S. 218 ff.
Schaar Peter	Biometrie und Datenschutz, „Adlershofer Kolloquium“ vom 28.06.2005, http://www.bfd.bund.de/aktuelles/akt20050628.pdf
Scheuermann Dirk	Digitale Ausweise – Möglichkeiten und Empfehlungen aus technischer Sicht, DuD 2005, S. 66 ff.
Sietmann Richard	Chipkarte mit Fingerabdruck, Kompetenzgerangel um neue biometrische Systemstandards, c't 23/2002
Strasser Peter	Die Vermessung des Verbrechermenschen, digma 2005, S. 162 ff.
TeleTrustDeutschland E.V. (Hrsg.)	Kriterienkatalog, Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren, Version 2.0 (Stand: EV. (Hrsg. 10.07.2002), Erfurt 2002, http://www.teletrust.de/fileadmin/files/kritkat_2-0.zip
Thalheim Lisa Krissler Jan Ziegler Peter-Michael	Körperkontrolle, Biometrische Zugangssicherungen auf die Probe gestellt, c't 11/2002
Walter Jean-Philippe	Referat "Quelques aspects de portection des données lors de l'utilisation de données biométriques dans le secteur privé", gehalten an der 26e Conférence internationale des Commissaires à la protection des données et à la vie privée, Wroclaw, 14 – 16 septembre 2004
Weichert Thilo	Biometrie – Freund oder Feind des Datenschutzes?, CR 1997, S. 369 ff.
Derselbe	Überwachung: Einblick in die Praxis, Gängige Überwachungspraktiken im Bereich des öffentlichen und des privaten Lebens, digma 2002, S. 4 ff.
Derselbe	Angriff auf den Datenschutz? Biometrieausweise fördern grundsätzliche Rechtsänderungen c't 2005, Heft 1, S. 94 ff.
Wirz Brigitte	Biometrische Verfahren, Überblick, Evaluierung und aktuelle Themen, DuD 1999, S. 129 ff.
Wollweber Harald	Datenschutz im Melde-, Ausweis- und Passwesen, in: Rossnagel Alexander (Hrsg.), Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003, S. 1517 ff.

Datenschutzkommission des Kantons Aargau

lic. iur. Gunhilt Kersten, Präsidentin
Bahnhofplatz 11, 5201 Brugg
Telefon 056 460 60 00
kersten@mhl.ch

Datenschutzbeauftragter des Kantons Appenzell A.Rh.

Dr. iur. Urs Glaus, Rechtsanwalt
Unterstrasse 15, 9001 St. Gallen
Telefon 071 222 10 20
info@gj-anwaelte.ch

Datenschutzaufsicht des Kantons Appenzell I.Rh.

lic. iur. Werner Niederer
Triangelstrasse 3, Postfach, 9101 Herisau
Telefon 071 351 55 84
w-k.niederer@swissonline.ch

Datenschutzbeauftragte des Kantons Basel-Landschaft

lic. iur. Ursula Stucki
Rathausstrasse 45, 4410 Liestal
Justiz-, Polizei- und Militärdirektion,
Postfach, 4410 Liestal
Telefon 061 925 64 30
datenschutz@jpm.bl.ch
www.baselland.ch/datenschutz

Datenschutzbeauftragter Basel-Stadt

Jean-Louis Wanner
Martinsgasse 16, Basel
Postfach 1249, 4001 Basel
Telefon 061 267 60 12
Jean-Louis.Wanner@bs.ch

Datenschutzbeauftragter des Kantons Bern

Markus Siegenthaler, Fürsprecher
Münstergasse 2, 3011 Bern
Telefon 031 633 76 10
markus.siegenthaler@jgk.be.ch
www.be.ch/dsa

Kantonale Aufsichtsstelle für Datenschutz Freiburg

Dominique Nouveau Stoffel, Datenschutzbeauftragte
Reichengasse 26, Postfach, 1701 Freiburg
Telefon 026 322 50 08
nouveaud@fr.ch
www.fr.ch/sprd

Commission de contrôle de l'informatique de l'Etat de Genève

3 Place de Bourg-de-Four, 1204 Genève
Telefon 022 327 00 76
CCIE@justice.ge.ch

Datenschutzbeauftragter des Kantons Glarus

lic. iur. Manfred Arm
Rathaus, 8750 Glarus
Telefon 055 646 69 62
manfred.arm@gl.ch

Datenschutzbeauftragter der kantonalen Verwaltung des Kantons Graubünden

lic. iur. Thomas Casanova, Rechtsanwalt
Arcas 22, 7002 Chur
Telefon 081 250 79 40
datenschutzbeauftragter@staka.gr.ch

Commission cantonale de la protection des données, Jura

Jean Moritz, Président
Le Château, 2900 Porrentruy
Telefon 032 465 33 00
jean.moritz@jura.ch

Datenschutzbeauftragter des Kantons Luzern

Dr. iur. Amédéo Wermelinger
Bahnhofstrasse 15, 6002 Luzern
Telefon 041 228 66 06
dsb@lu.ch
www.datenschutz.lu.ch

Autorité de surveillance en matière de protection de la personnalité du canton de Neuchâtel

Laurent Margot, Président du Tribunal du district du Val-de-Travers
Greffes du Tribunal, Grande-Rue 10, 2112 Môtiers
Telefon 032 889 61 89
protectiondesdonnees@ne.ch
www.ne.ch/protectiondesdonnees

Datenschutzkommission des Kantons Nidwalden

Rolf Brühwiler
Regierungsgebäude, 6370 Stans
Dorfplatz 2, 6371 Stans
Telefon 041 618 79 12
rolf.bruehwiler@nw.ch

Datenschutzbeauftragter des Kantons Obwalden

André Blank
Polizeigebäude, 6060 Sarnen
Postadresse
Postfach, 6061 Sarnen
Telefon 041 666 63 67
justizverwaltung@ow.ch

Datenschutzbeauftragter des Kantons Schaffhausen

Rechtsanwalt lic. iur. Christoph Storrer
Vorstadt 18, 8200 Schaffhausen
Telefon 052 632 20 64
storrersh@bluewin.ch

Datenschutzkommission des Kantons Schwyz

Richard Carletti, Geschäftsführer
Bahnhofstrasse 15, 6431 Schwyz
Postadresse
Postfach 1234, 6431 Schwyz
Telefon 041 819 23 15
richard.carletti@sz.ch

Informations- und Datenschutzbeauftragter des Kantons Solothurn

Daniel Schmid
Rathaus, Barfussergasse 24, 4509 Solothurn
Telefon 032 627 26 82
daniel.schmid@sk.so.ch
www.datenschutz.so.ch

Datenschutzbeauftragte des Kantons St. Gallen

lic. rer. publ. Corinne Suter,
Juristische Mitarbeiterin im Rechtsdienst der Staatskanzlei
Regierungsgebäude, 9001 St. Gallen
Telefon 071 229 32 62
corinne.suter@sg.ch
www.sg.ch/home/sicherheit/datenschutz.html

Datenschutzbeauftragter des Kantons Thurgau

Ernst Frei
Finanzkontrolle/Datenschutz, Kasernenplatz 4,
8500 Frauenfeld
Telefon 052 724 27 11
ernst.frei@kttg.ch

**Responsabile per la protezione
dei dati del Cantone Ticino**

Dr. iur. Michele Albertini
Residenza governativa, Piazza Governo, 6500 Bellinzona
Telefon 091 814 45 02 (Sekretariat)
protezionedati@ti.ch
www.ti.ch/protezionedati

Datenschutzbeauftragte des Kantons Uri

lic. iur. Beatrice Kolvodouris Janett
Lehnplatz 11, 6460 Altdorf
Telefon 041 872 03 33
datenschutz@ur.ch

**Secrétariat général du Département
des finances du Canton de Vaud**

Sophie Hornung
Rue de la Paix 6, 1014 Lausanne
Telefon 021 316 20 10
sophie.hornung@sg-dfin.vd.ch

**Commission cantonale de la protection
des données, Valais**

Jean-Paul Salamin, avocat et notaire, Président
Sekretariat
Claude Bumann, Chef du Service parlementaire
Grand-Pont 4, C.P. 478, 1951 Sion
Telefon 027 606 21 87
CCPD@admin.vs.ch
www.vs.ch/Navig/navig.asp?MenuID=2712

Datenschutzbeauftragter des Kantons Zug

Dr. iur. René Huber
Regierungsgebäude, Postplatz, 6300 Zug
Postadresse
Postfach 156, 6301 Zug
Telefon
Sekretariat: 041 728 31 47
René Huber: 041 728 31 87
rene.huber@allg.zg.ch
www.datenschutzzug.ch

Datenschutzbeauftragter des Kantons Zürich

Dr. Bruno Baeriswyl
Kaspar Escher-Haus, 8090 Zürich
Telefon 043 259 39 99
datenschutz@dsb.zh.ch
www.datenschutz.ch

Datenschutzaufsicht der Gemeinde Belp

Gemeindeverwaltung Belp
Datenschutzbeauftragter
Gartenstrasse 2, 3123 Belp
datenschutz@belp.ch

Datenschutzbeauftragter der Stadt Dietikon

Guido Solari
Bremgartnerstrasse 22, 8953 Dietikon
Telefon 044 744 36 26
guido.solari@dietikon.ch
www.dietikon.ch

**Datenschutzbeauftragter / Stabsstelle für Datenschutz
der Liechtensteinischen Landesverwaltung**

Dr. Philipp Mittelberger
Äulestrasse 51, Postfach 684, 9490 Vaduz/FL
Telefon 00423 236 60 91
info@sds.llv.li
www.sds.llv.li (Verwaltung)
www.liechtenstein.li (Liechtenstein)

Datenschutzbeauftragter der Einwohnergemeinde Steffisburg

Stöckli Rechtsanwälte
Kurt Stöckli
Schwanengasse 5/7, 3001 Bern
Telefon 031 326 51 71
ks@stoeckli-rechtsanwaelte.ch
www.stoeckli-rechtsanwaelte.ch

Datenschutzbeauftragter der Stadt Thun

Stöckli Rechtsanwälte
Kurt Stöckli
Schwanengasse 5/7, 3001 Bern
Telefon 031 326 51 71
ks@stoeckli-rechtsanwaelte.ch
www.stoeckli-rechtsanwaelte.ch

Datenschutzbeauftragter der Stadt Zürich

Marcel Studer
Röslistrasse 11, 8006 Zürich
Telefon 01 363 24 42
info@das.stzh.ch
www.das.stzh.ch

Impressum

Herausgeber

privatim
die schweizerischen datenschutzbeauftragten
les commissaires suisses à la protection des données

Bezug

Kantonale Aufsichtsstelle für Datenschutz
Reichengasse 26, Postfach, 1701 Freiburg
nouveaud@fr.ch

Gestaltung

konkret – visuelle kommunikation, luzern
www.diekonkreten.ch

Druck

Eicher Druck, Horw
www.eicherdruck.ch

Auflage

500 Exemplare

Version

1.0, Oktober 2006

Preis

Fr. 38.– (plus Porto)

ISBN

978-3-033-00941-7

