

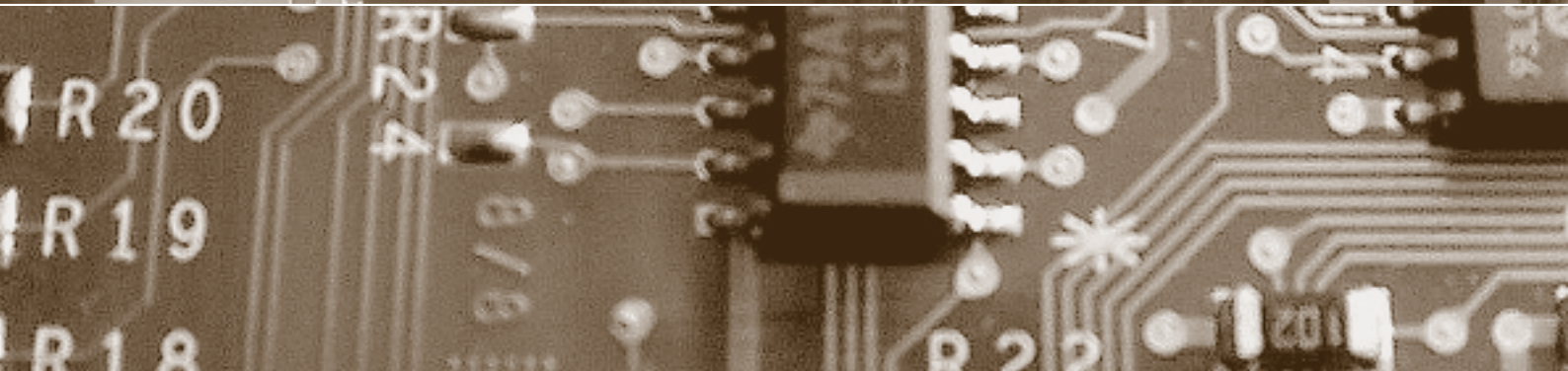
Schwerpunkt:

## Biometrie

**fokus:** Der menschliche Körper als Datenträger

**fokus:** Die Vermessung des Verbrechermenschen

**report:** Das «Spam-Urteil» der EDSK



Herausgegeben von  
**Bruno Baeriswyl**  
**Beat Rudin**  
**Bernhard M. Hämmerli**  
**Rainer J. Schweizer**  
**Michael Waidner**

## fokus



### Schwerpunkt: **Biometrie**

auftakt

Der Rechtsstaat auf der  
Bewährungsprobe

von Claude Janiak

**Seite 145**

Der maschinenlesbare Mensch  
von Beat Rudin

**Seite 148**

Der menschliche Körper als Datenträger

von Klaus Peter Rippe

**Seite 150**

Biometrie – wie einsetzen und  
wie nicht?

von Andreas Pfitzmann

**Seite 154**

Der Einsatz biometrischer Systeme

von Beda Harb/ Daniel Schmid

**Seite 158**

Die Vermessung des Verbrechermenschen

von Peter Strasser

**Seite 162**

Die Balance zwischen Freiheit und Sicherheit zu finden, mag, zumal in Zeiten terroristischer Angriffe auf den liberalen Rechtsstaat, schwierig sein. Der Gesetzgeber – so mahnt der Nationalratspräsident – darf die Freiheit der Bürgerinnen und Bürger nicht leichtfertig aufs Spiel setzen.

**Der Rechtsstaat auf der Bewährungsprobe**

Was ist neu am «Festmachen von Daten» am Körper? Verändert die Nähe etwas im Verhältnis zum Menschen und seinem Körper? Welche Fragen stellen sich aus philosophischer und ethischer Sicht?

**Der menschliche Körper als Datenträger**

Biometrie wird als Lösung vieler Zugangskontrollprobleme angepriesen. Sie hat aber nicht nur Sicherheitsprobleme, sondern verursacht auch gravierende Sicherheitsprobleme. Was kann Biometrie, was nicht, und welche Gestaltungsaufgaben stellen sich?

**Biometrie – wie einsetzen und wie nicht?**

Die Entwicklung der Menschenvermessung – von den «Körperlesern» über die «Psychojäger» bis heute – führt von der Makro- zur Mikrokontrolle. Abweichung soll erkannt werden: auf der neurologischen Ebene des Gehirns, im Molekularbereich des Genoms und mit einem feinmaschigen Überwachungsnetz, das die Gesellschaft sanft überzieht.

**Die Vermessung des Verbrechermenschen**

## impresum

**digma:** Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 13239944, Website: [www.digma.info](http://www.digma.info)

**Herausgeber:** Dr. iur. Bruno Baeriswyl, Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. Dr. iur. Rainer, J. Schweizer, Dr. Michael Waidner

**Redaktion:** Dr. iur. Bruno Baeriswyl und Dr. iur. Beat Rudin

**Rubrikenredaktor:** Dr. iur. Amédéo Wermelinger

**Zustelladresse:** Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Kirschgartenstrasse 7, CH-4010 Basel  
Tel. +41 (0)61 270 17 70, [redaktion@digma.info](mailto:redaktion@digma.info)

**Erscheinungsplan:** jeweils im März, Juni, September und Dezember

**Abonnementspreise:** Jahresabo Schweiz: CHF 155.00, Jahresabo Ausland: Euro 126.00 (inkl. Versandkosten), Einzelheft: CHF 42.00

**Anzeigenmarketing:** Schulthess Druck AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich  
Tel. +41 (0)44 383 66 50, Fax +41 (0)44 383 79 45

**Druck:** Schulthess Druck AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich, ISDN +41 (0)44 383 66 50

**Verlag und Abonnementsverwaltung:** Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich  
Tel. +41 (0)44 200 29 19, Fax +41 (0)44 200 29 08, [www.schulthess.com](http://www.schulthess.com), [zs.verlag@schulthess.com](mailto:zs.verlag@schulthess.com)

## Datenschutzfreundliche Missbrauchs-entdeckung

Die Analyse eines Systems bei Missbrauchsverdacht erfordert Audit-Daten, die oft personenbezogene Merkmale enthalten. Eine Analyse ist datenschutzkonform möglich, wenn die Daten so pseudonymisiert werden, dass sie zu vorab definierten Zwecken analysiert werden können und Pseudonyme nur unter vorab spezifizierten Bedingungen aufdeckbar sind.

## RFID: Datenschutzprobleme und -lösungen

RFID wird in Bibliotheken oder in der Warenlogistik, aber auch zur Identifikation hochwertiger Güter oder zur Personenidentifizierung eingesetzt. Dadurch entstehen Konflikte mit dem Datenschutz, etwa wegen der Gefahr des unbefugten Auslesens. Wie lässt sich dieses Problem lösen?

## Unverlangt zugestellte Werbemails («Spam»)

Die EDSB hält in einem neuen Urteil fest: E-Mail-Adressen – selbst Phantasiebezeichnungen – sind Personendaten. Und wer per E-Mail massenweise und unverlangt Streuwerbung versendet, begeht eine widerrechtliche Persönlichkeitsverletzung.

## Wireless LAN – aber sicher

Immer mehr User nützen Wireless LAN, im Büro, zu Hause oder unterwegs. Peter Heinzmann und Andreas Steffen unterhalten sich mit einem Gast über die Risiken des WLAN- Einsatzes.

## report



### TECHNIK

Datenschutzfreundliche Missbrauchs-entdeckung

von Ulrich Flegel

**Seite 168**

### TECHNIK

RFID: Sicherheitsprobleme und -lösungen

von Stephan Lechner

**Seite 172**

### RECHTSPRECHUNG

Unverlangt zugestellte Werbemails («Spam»)

redigiert von Beat Rudin

**Seite 176**

### RECHTSPRECHUNG

Der Vertrauensarzt der Krankenkasse

von Amédéo Wermelinger

**Seite 184**

### RECHTSPRECHUNG

Nochmals zur Öffentlichkeit eines Audits

von Amédéo Wermelinger

**Seite 186**

### BRÜCKENSCHLAG

Wireless LAN – aber sicher

Gast: Thomas Rudin

**Seite 188**

## forum



### BUCHBESPRECHUNG

Grundrechtsschutz und genetische Informationen (Claudia Mund)

von Beat Rudin

**Seite 190**

### DSB+CPD.CH

Klare strategische Ausrichtung

von Bruno Baeriswyl

**Seite 191**

### KONFERENZ

Polizei-Zusammenarbeit im föderalen Staat

von René Huber

**Seite 192**

agenda

**Seite 195**

schlussstakt

**Seite 196**

cartoon

von Hanspeter Wyss

# Der Einsatz biometrischer Systeme

Verfassungsrechtliche Aspekte und Umsetzung der datenschutzrechtlichen Anforderungen beim Einsatz von Biometrie



lic. iur. Beda Harb, Stellvertreter des Datenschutzbeauftragten des Kantons Zürich, Zürich  
datenschutz@dsb.zh.ch

**Der Einsatz biometrischer Systeme ist im Trend. Doch nicht jeder Einsatz ist verfassungs- und datenschutzkonform. Was ist zu beachten?**

Mit dem Erfassen, Speichern und Abgleichen von biometrischen Daten greifen sowohl Private als auch der Staat in die Grundrechte der Bürgerinnen und Bürger ein. Grundrechte dürfen jedoch nur eingeschränkt werden, wenn eine gesetzliche Grundlage besteht, ein öffentliches Interesse vorliegt oder Grundrechte Dritter geschützt werden müssen und wenn der Eingriff verhältnismässig ist. Dabei ist aber deren Kerngehalt unantastbar<sup>1</sup>.

## Verfassungsrechtliche Aspekte

Bei der Bearbeitung biometrischer Daten werden vor allem folgende Grundrechte tangiert: Menschenwürde, persönliche Freiheit (Bewegungsfreiheit), Privatsphäre und das Recht auf informationelle Selbstbestimmung<sup>2</sup>. Eine besondere Bedeutung erlangt dabei die Menschenwürde. Die Menschenwürde ist Kern und Grundgehalt anderer Grundrechte<sup>3</sup>. «Die Würde des Menschen ist zu achten und zu schützen» (Art. 7 BV). Kernaussage der Menschenwürde ist, dass der Mensch nicht als «Objekt», «Nummer» oder «Ware» behandelt werden darf<sup>4</sup>. Die Menschenwürde darf nicht eingeschränkt werden, selbst nicht bei Krieg oder anderen Gefahren für das Überleben des Staates<sup>5</sup>.

Der Einsatz biometrischer Verfahren ist nicht per se menschenunwürdig, also verfassungswidrig. Vielmehr muss bei der jeweiligen konkreten Anwendung geprüft werden, ob die Menschenwürde oder der Kerngehalt der erwähnten Grundrechte verletzt werden oder nicht. Bei den zwei folgenden Beispielen liegt ein Verstoss gegen die Menschenwürde im Sinne von Art. 7 BV vor:

■ Beispiel 1: Flächendeckender Einsatz biometrischer Daten als Personenidentifikator.

Biometrische Daten werden als Bindeglied – analog einer Kennziffer – zur Verknüpfung verschiedenster Datenbanken und der darin gespeicherten (z.T. besonders schützenswerten) Personendaten verwendet. Mittels der erstellten Verknüpfungen können sowohl Behörden wie auch Private, welchen der Zugriff gewährt wird, Persönlichkeitsprofile erstellen, welche nahezu jeden Lebensbereich abdecken.

■ Beispiel 2: Bearbeitung biometrischer Daten in einer zentralen, alle Einwohner(innen) der Schweiz umfassenden Datenbank ohne Zweckbindung, auf unbestimmte Zeit und ohne Zugriffsbeschränkungen bzw. mit fortlaufender Ausdehnung der Zugriffsberechtigungen. Biometrische Daten werden für verschiedenste Zwecke verfügbar und ihre Verwendung wird damit unkontrollierbar. Eine solche Speicherung biometrischer Daten stellt eine Vorratsdatenspeicherung dar, welche den unantastbaren Kerngehalt des informationellen Selbstbestimmungsrechts verletzt<sup>6</sup>. Verfassungswidrig wäre etwa die Schaffung einer DNA-Datenbank aller Einwohner(innen) im beschriebenen Rahmen.

Die beiden Beispiele zeigen verfassungswidrige Anwendungen. Konkrete Einzelanwendungen werden häufig für sich alleine betrachtet vor der Verfassung Stand halten können. Der Einsatz biometrischer Systeme darf in der Gesamtheit aber nicht dazu führen, dass die bisher geltende Privatheit und Anonymität in weiten Teilen unseres täglichen Lebens aufgehoben wird. In diesem Sinne ist jede Einzelanwendung auch im Gesamtzusammenhang zu würdigen, im Sinne eines Steinchens des Mosaiks.

## Datenschutzrechtliche Aspekte

Die datenschutzrechtlichen Aspekte sollen an einem Anwendungsbeispiel konkretisiert werden, bei welchem aus verfassungsrechtlicher Sicht kaum Schranken gesetzt sind: Die Berechtigung zum Eintritt soll bei Inhaber(inne)n von Saison- und Jahresabonnements eines kommunalen Schwimmbades mittels ihres Fingerabdruckes geprüft werden.



lic. iur. Daniel Schmid, Beauftragter für Information und Datenschutz des Kantons Solothurn, Solothurn  
daniel.schmid@sk.so.ch

## Rechtsgrundlage

Jede Bearbeitung von Personendaten durch staatliche Organe bedarf einer gesetzlichen Grundlage; die Bearbeitung besonders schützenswerter Personendaten ist in einem Gesetz im formellen Sinn zu regeln<sup>7</sup>. Personendaten sind «alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen»<sup>8</sup>. Biometrische Daten lassen für sich allein betrachtet Rückschlüsse auf eine bestimmte Person zu; sie sind körpereigene, einmalige<sup>9</sup> Kennzeichen und untrennbar mit einer bestimmten Person verknüpft.

Unseres Erachtens sind biometrische Daten nicht automatisch<sup>10</sup> besonders schützenswerte Personendaten, sondern nur unter bestimmten Voraussetzungen, z.B.

- auf Grund ihrer Verwendung, etwa in einem Strafverfahren,
- sofern mit ihrer Hilfe Persönlichkeitsprofile erstellbar sind,
- soweit technisch möglich, eindeutige Rückschlüsse auf körperliche, charakterliche Eigenschaften, Gesundheit, Rasse/Ethnie möglich sind,
- oder wenn das Datenschutzgesetz den Katalog der besonders schützenswerten Personendaten nicht abschliessend aufzählt<sup>11</sup>.

Die Verwendung eines Fingerabdruckes für die Autorisierung beim Eintritt in ein Schwimmbad stellt keine Bearbeitung besonders schützenswerter Personendaten dar. Es genügt deshalb, dass eine Grundlage für den Betrieb des Schwimmbades in einem Gesetz oder einer Verordnung besteht. Daraus ergibt sich die Kompetenz, die zur Erfüllung dieser Aufgabe notwendigen Personendaten zu bearbeiten.

## Verhältnismässigkeit

Das Bearbeiten von Personendaten muss für die Erfüllung einer Aufgabe geeignet und erforderlich sein<sup>12</sup>. Da jede Bearbeitung von Personendaten einen Eingriff in das informationelle Selbstbestimmungsrecht darstellt, bedarf sie einer besonderen Begründung; Kundenfreundlichkeit oder Bequemlichkeit genügen dafür nicht. Eine Identifikation oder Verifikation darf nur vorgenommen werden, soweit sie im konkreten Anwendungsfall begründet ist.

Auf Besitz oder Wissen beruhende Verfahren zur Autorisierung beim Schwimmbadeintritt können leicht umgangen werden; Missbräuche können erhebliche Einnahmeherausfälle zur Folge haben. Es erscheint deshalb grundsätzlich verhältnismässig, ein biometrisches Merkmal für diesen Zweck

einzusetzen; der Fingerabdruck erscheint geeignet.

Für die Autorisierung genügt ein biometrisches Merkmal; der Name der Person oder weitere Angaben wie Geburtsdatum oder Adresse sind dafür nicht erforderlich. Aus dem Verhältnismässigkeitsgrundsatz folgt auch,

## Der Eingriff in das informationelle Selbstbestimmungsrecht bedarf einer besonderen Begründung; Kundenfreundlichkeit oder Bequemlichkeit genügen dafür nicht.

dass Rohdaten ohne besondere Begründung nur zur Erzeugung von Templates<sup>13</sup> zu verwenden sind. Die heute zur Verfügung stehende Technik erlaubt es, dass die betroffene Person einzelne Bearbeitungsvorgänge in der unter ihrer Kontrolle stehenden Sphäre ausführt. Es ist deshalb für jeden Schritt eines biometrischen Verfahrens separat zu prüfen, ob die Bearbeitung zwingend durch das öffentliche Organ vorgenommen werden muss.

Für die Autorisierung beim Schwimmbadeintritt bedeutet dies, dass aus dem Fingerabdruck ein Template zu erstellen ist; Rohdaten werden nicht weiter benötigt. Das Template ist auf einer bei der betroffenen Person verbleibenden Smartcard abzulegen und beim Wiedereintritt mit dem erzeugten Prüfmuster zu vergleichen. Aus datenschutzrechtlicher Sicht noch besser sind Systeme, bei denen auch das Einlesen des Fingerabdrucks und der Verifizierungsvorgang in der Nutzersphäre stattfinden. Biometrische Daten sind nicht bei der Schwimmbadbetreiberin abzulegen; damit obliegt dieser auch keine entsprechende Verantwortung.

Besondere Beachtung ist dem Verhältnismässigkeitsgrundsatz bei der Bearbeitung

### Kurz und bündig

Wie jede andere Datenbearbeitung muss der Einsatz jedes biometrischen Systems durch ein staatliches Organ den verfassungs- und datenschutzrechtlichen Grundsätzen genügen. Der Einsatz eines oder einer Vielzahl von biometrischen Systemen darf nicht dazu führen, dass bisher anonymes und privates Verhalten in weiten Lebensbereichen nicht mehr möglich ist. Es ist möglich,

eine rechtskonforme Lösung der Autorisierung beim Schwimmbadeintritt mit Hilfe eines biometrischen Systems umzusetzen. Dem Verhältnismässigkeitsprinzip ist bei der Personenerkennung wie auch bei der Speicherung und späteren Auswertung von Randdaten besondere Beachtung zu schenken. Das Zweckbindungsgebot wird vorab auf der technischen Ebene umgesetzt.

personenbezogener Randdaten zu schenken. Die Prinzipien der Datenvermeidung, der Datensparsamkeit sowie der Pseudonymisierung und Anonymisierung gelten nicht nur für die maschinelle Erkennung von Personen, sondern auch bei der Speicherung und späteren Auswertung der Resultate. Nicht mehr benötigte Daten sind zu vernichten, sofern sie nicht der Archivbehörde zuzustellen sind<sup>14</sup>.

### Zweckbindung

Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Erhebung oder Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist<sup>15</sup>. Die technische Lösung ist darauf auszurichten, dass der Zweck der Datenbearbeitung

ist zur Erfassung der Rohdaten und Erzeugung von Templates und Prüfmustern eine geschlossene Kompakteinheit zu verwenden. Es ist ein anwendungsspezifischer Algorithmus einzusetzen, der aus den Templates weder eine Wiederherstellung der Rohdaten noch Rückschlüsse auf Charaktereigenschaften oder eindeutige medizinische Diagnosen zulässt. Die Einhaltung der Zweckbindung ist bei personenbezogenen Randdaten durch enge Fassung und entsprechende technische Umsetzung des Verhältnismässigkeitsprinzips sicherzustellen.

### Richtigkeit

Biometrische Daten müssen richtig und soweit es der Zweck des Bearbeitens verlangt, aktuell und vollständig sein<sup>16</sup>. Es dürfen deshalb nur biometrische Verfahren eingesetzt werden, welche eine nahezu 100%ige Sicherheit der Identifikation oder Verifikation erlauben. Für Personen, die auf dem System nicht eingelernt werden können, ist ein Alternativszenario, welches nicht zu einer Diskriminierung führen darf, vorzusehen.

Beim Schwimmbad-Eintritt kann eine falsche Zulassung einer Person mit dem Verdacht einer strafbaren Handlung verbunden sein, eine falsche Nichtzulassung mit Ärger und finanziellen Folgen.

## Datenschutzrechtliche Aspekte sind bereits bei der Evaluation und Planung eines Systems zu berücksichtigen.

erreicht, eine Änderung des ursprünglichen Bearbeitungszweckes aber möglichst ausgeschlossen wird. Datenschutzrechtliche Aspekte sind deshalb bereits bei der Evaluation und Planung eines Systems zu berücksichtigen. So

### Fussnoten

<sup>1</sup> Art. 36 der Schweizerischen Bundesverfassung vom 18. April 1999 (BV, SR 101).

<sup>2</sup> Art. 7, Art. 10 Abs. 2 und Art. 13 BV.

<sup>3</sup> PHILIPPE MASTRONARDI, St. Galler Kommentar zu Art. 7 BV, Rz 28.

<sup>4</sup> PHILIPPE MASTRONARDI, a.a.O. zu Art. 7 BV, Rz 43–45 mit Beispielen aus der Rechtspraxis, zum allgemeinen Gehalt der Menschenwürde siehe auch BGE 127 I 6 ff. E. 5b sowie Urteil des deutschen Bundesverfassungsgerichts 1 BvR 2378/98 vom 03.03.2004 über den «grossen Lauschangriff» in <[http://www.bverfg.de/entscheidungen/rs20040303\\_1bvr237898.html](http://www.bverfg.de/entscheidungen/rs20040303_1bvr237898.html)> (31.10.2005).

<sup>5</sup> Art. 15 EMRK, Art. 4 UNO-Pakt II, Art. 3 des Genfer Abkommens über die Behandlung der Kriegsgefangenen, PHILIPPE MASTRONARDI, a.a.O. zu Art. 7 BV, Rz 52.

<sup>6</sup> Art. 13 Abs. 2 BV; Das Bundesgericht hat bereits unter der alten BV ein ungeschriebenes Grundrecht auf informationelle Selbstbestimmung anerkannt (vgl. BGE 113 Ia 1, 113 Ia 257, RAINER J. SCHWEIZER, St.Galler Kommentar zu Art. 13 BV, Rz 38 mit Hinweisen auf weitere Bundesgerichtsurteile).

<sup>7</sup> Personendaten: Art. 17 Abs. 1 des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (DSG, SR 235.1), § 4 Abs. 1 des Gesetzes vom 6. Juni 1993 über den Schutz von Personendaten des Kantons Zürich (DSG ZH, LS 236.1), § 15 Abs. 1 Bst. a des Informations- und Datenschutzgesetzes vom 21. Februar 2001 des Kantons Solothurn (InfoDG SO, BGS 114.1); besonders schützenswerte Personendaten: Art. 17 Abs. 2 DSG, § 5 Bst. a DSG ZH, § 15 Abs. 2 Bst. a InfoDG SO.

<sup>8</sup> Art. 3 Bst. a DSG.

<sup>9</sup> Einmaligkeit verlangt eine nahezu 100%ige Sicherheit, dass es sich um die bestimmte Person handelt.

<sup>10</sup> Auf eine andere Auffassung, wonach biometrische Daten automatisch besonders schützenswerte Personendaten sind, wird im Rahmen dieses Beitrages nicht näher eingegangen.

<sup>11</sup> So sind etwa gemäss § 2 Bst. d DSG ZH. Besonders schützenswerte Personendaten «Daten, bei denen wegen ihrer Bedeutung, der Art ihrer Bearbeitung oder ihrer Verknüpfung mit anderen Daten eine besondere Gefahr einer Persönlichkeitsverletzung besteht, wie Daten über...».

<sup>12</sup> Art. 4 Abs. 2 DSG, § 4 Abs. 3 DSG ZH, § 16 Abs. 1 Bst. a, InfoDG-SO.

<sup>13</sup> In einem biometrischen Verfahren wird ein spezielles Muster-generierungs- oder Mustererkennungsverfahren eingesetzt und aus dem Merkmal ein Muster (Template) des Abdrucks des personengebundenen Merkmals generiert. Dazu wird ein spezieller Algorithmus eingesetzt.

<sup>14</sup> Art. 21 DSG, § 14 DSG ZH, § 19 InfoDG SO.

<sup>15</sup> Art. 4 Abs. 3 DSG, § 4 Abs. 4 DSG ZH, § 16 Abs. 2 InfoDG SO.

<sup>16</sup> Art. 5 DSG, § 4 Abs. 2 DSG ZH, § 16 Abs. 1 Bst. b InfoDG SO.

<sup>17</sup> Art. 4 Abs. 2 und 18 DSG, § 7 Abs. 1 DSG ZH, §§ 16 Abs. 1 Bst. a und 18 InfoDG SO.

<sup>18</sup> Art. 8 ff. DSG, §§ 17 ff. DSG ZH, §§ 26 ff. InfoDG SO.

<sup>19</sup> Art. 7 DSG, § 4 Abs. 5 DSG ZH, § 16 Abs. 1 Bst. c InfoDG SO.

<sup>20</sup> Art. 16 DSG, § 6 Abs. 1 DSG ZH.

### Transparenz

Personendaten müssen in der Regel bei der betroffenen Person erhoben werden. Ausnahmen bedürfen einer Rechtsgrundlage<sup>17</sup>. Ein Teil der biometrischen Merkmale kann ohne Wissen und Willen der betroffenen Person erfasst werden; dies ist nicht zulässig. Das Gebot der Transparenz gilt auch bei der Übermittlung von Personendaten. Besondere – nicht biometrie-spezifische – Fragestellungen ergeben sich daraus infolge der neuen Funktechnologien.

### Rechte der betroffenen Person

Die den betroffenen Personen gewährten Rechte<sup>18</sup> sind auch bei der Bearbeitung von Personendaten mittels biometrischer Systeme uneingeschränkt zu gewährleisten.

### Datensicherheit

Daten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt wer-

den<sup>19</sup>. Ein biometrisches System muss zudem eine hohe Ausfallsicherheit aufweisen, da der Vergleich von Template und Prüfmuster nicht manuell durchgeführt werden kann. Das Risiko des Ausfalles des biometrischen Systems liegt bei der Betreiberin; es ist nicht zulässig, zusätzliche Personendaten zur Vermeidung dieses Risikos zu erfassen.

### Verantwortung

Für den Datenschutz ist das Organ verantwortlich, das die Personendaten zur Erfüllung seiner Aufgaben bearbeitet oder bearbeiten lässt<sup>20</sup>. Die Gemeinde als Schwimmbadbetreiberin kann sich ihrer Verantwortung nicht entziehen. Die Marktdurchsetzung eines biometrischen Systems hängt nicht nur von Kosten, Wahrscheinlichkeiten und Benutzerfreundlichkeit ab. Die Einhaltung der verfassungs- und datenschutzrechtlichen Rahmenbedingungen steigert die Akzeptanz – und ist aus rechtlicher Sicht unabdingbar. ■

d i g m a

– Schriften zum Datenrecht

Herausgegeben von Bruno Baeriswyl und Beat Rudin

## Herausforderung Datenschutz

### 10 Jahre Datenschutzgesetz – eine Zwischenbilanz

Datenschutzbeauftragter des Kantons Zürich (Hrsg.)

2005. 99 Seiten, broschiert, CHF 45.– (Band 1)

Die Informations- und Kommunikationsgesellschaft stellt neue Anforderungen an den Schutz der Privatheit der Bürgerinnen und Bürger. Das Datenschutzrecht steht im Zentrum einer technologischen und gesellschaftlichen Entwicklung, bei der die Regelung des Zugangs und des Schutzes von Informationen hohe Anforderungen an den Gesetzgeber stellt. Die Erfahrungen mit dem Datenschutzrecht im Kanton Zürich, wie sie an einer Tagung präsentiert wurden, und die Einführung des Öffentlichkeitsprinzips sind Ausgangspunkte der Beiträge in diesem Band, die sich mit den aktuellen Herausforderungen für den Datenschutz befassen.



Schulthess §

Schulthess Juristische Medien AG, Postfach, 8022 Zürich, Telefon 044 200 29 29, Fax 044 200 29 28  
E-Mail: buch@schulthess.com, Homepage: www.schulthess.com

## Meine Bestellung

- 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)  
à **CHF 155.00** bzw. bei Zustellung ins Ausland **EUR 126.00** (inkl. Versandkosten)

Name \_\_\_\_\_ Vorname \_\_\_\_\_

Firma \_\_\_\_\_

Strasse \_\_\_\_\_

PLZ \_\_\_\_\_ Ort \_\_\_\_\_ Land \_\_\_\_\_

Datum \_\_\_\_\_ Unterschrift \_\_\_\_\_

### Bitte senden Sie Ihre Bestellung an:

Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8022 Zürich

Telefon +41 44 200 29 19

Telefax +41 44 200 29 18

E-Mail: [zs.verlag@schulthess.com](mailto:zs.verlag@schulthess.com)

Homepage: [www.schulthess.com](http://www.schulthess.com)