

Wir arbeiten an diesen Themen:

Flucht & Migration

- Die Visa Warndatei
- Das Entry-Exit System
- FRONTEX, die EU-Grenzschutzagentur
- Die europäische Fluggastdatenbank (PNR)
- Schengen-Informationssystem II



Polizei & Geheimdienste

- Vorratsdatenspeicherung VDS 2.0
- Video- und Lauschangriff auf Wohnungen
- Datenabgleich zwischen Polizei und Geheimdiensten (GTAZ)
- Das zentrale Bundesmelderegister BZR
- Rasterfahndung in zentralen Datenbanken
- Biometrische Daten im elektronischen Ausweis und Pass
- Keine Online Durchsuchung privater PCs, weg mit dem Staatstrojaner

SchülerInnen-Themen

- Kein Militär an Schulen
- Keine Drohnen für Krieg & Überwachung
- Zivilklauseln an die Unis
- Baby-Datei, Schüler-Datei
- Persönlichkeitsprofile, lebenslang abgestempelt

Verbraucher- und ArbeitnehmerInnen-Datenschutz

- Gläserner Bürger, Kundenkarten, Scoring
- Die elektronische Gesundheitskarte
- Für Datenschutz auch am Arbeitsplatz
- Gegen den elektronischen Einkommensnachweis ELENA ... und Nachfolger OMS
- Die bundeseinheitliche Steuernummer

Zensur & Informationsfreiheit

- Gegen Internetsperren und Zensur
- Für Netzneutralität & Informationsfreiheit
- Stopp ACTA – TAFTA – CETA & TTIP
- Open Source statt Kommerzialisierung

Verteidigen wir gemeinsam unser Grundgesetz, unser Recht auf informationelle Selbstbestimmung und die Menschenwürde!

Jede/r kann mitmachen und sich mit uns für seine Bürgerrechte einsetzen.

Die nächsten Termine unserer regelmäßigen Treffen im Berliner Antikriegs-Café COOP, Rochstr. 3, Nähe Alexanderplatz, werden auf unseren Webseiten unter dem Punkt **Aktivengruppen** angekündigt.

Aktion Freiheit statt Angst e.V.
Rochstr. 3,
D-10178 Berlin

Mail: kontakt@aktion-fsa.de
Web: aktion-freiheitstattangst.org



**AKTION
Freiheit
statt
Angst**

*Für Freiheitsrechte, gegen
Massen-Überwachung und Sicherheitswahn*

Spendenkonto:

Aktion Freiheit statt Angst e.V.
Triodos Bank
IBAN: DE72 5003 1000 1060 9910 02
BIC: TRODDF1

Der Verein ist ab 01.01.2011 nach §§ 52 1(2) Nr. 24 AO als gemeinnützig anerkannt, Spenden sind steuerlich absetzbar.

Dieser Flyer wurde gefördert durch den AstA der Universität Potsdam



**AKTION
Freiheit
statt
Angst**

Aktion Freiheit statt Angst e.V.

Für unsere Grundrechte, gegen Massen-Überwachung und Sicherheitswahn

*Mitglied im
European Civil Liberties Network*

Biometrische Daten auf RFID-Chips in Pässen und Ausweisen



Wo lauern die Gefahren?

Biometrische Daten in Pässen und Ausweisen

Seit Jahren werden in Deutschland ständig neue Gesetze zur „Verbesserung der Sicherheit“ eingeführt. Insbesondere nach den Anschlägen des 11. 9. 2001 wurde das deutsche Passrecht mehrmals geändert. Ziel war es, den Reisepass und inzwischen auch den Personalausweis sicherer zu machen. Das Gegenteil ist leider eingetreten.

In den neuen Ausweisdokumenten werden die Angaben zur Person sowie Gesichtsbild und Fingerabdrücke auf einem Chip elektronisch gespeichert. Dieser sogenannte RFID-Chip (Radio Frequency Identification) ist mittels Funktechnik auslesbar, d.h. es ist kein direkter Kontakt mit dem Pass notwendig. Je nach Qualität der eingesetzten Technik ist dies über 10cm oder auch über einige Meter möglich.

Wo lauern die Gefahren?

Bereits im Herbst 2010 hat der Chaos Computer Club (CCC) gezeigt, dass Fremde die Daten des neuen Personalausweises inkl. der PIN mitlesen und sogar ändern können. Dazu ist lediglich die notwendige kriminelle Energie und ein handelsüblicher Keylogger nötig. Hacker konnten in der Londoner U-Bahn die Pässe der Mitreisenden auslesen.

Davor wird auch in der Broschüre des Unabhängigen Landeszentrum für Datenschutz in Schleswig-Holstein (www.datenschutzzentrum.de) gewarnt, die jeder Bürger bei der Beantragung eines Passes erhält:

„Die Passdaten einschließlich biometrischer Angaben können nicht nur bei den Behörden, sondern bei Kenntnis der Daten der „Maschinenlesbaren Zone“ (MRZ) auch unbemerkt von unberechtigten Dritten ausgelesen werden, ...



... ist es möglich, den Ausweis elektronisch zu lesen, wenn der Passbesitzer diesen z.B. in der Hosen- oder Jackentasche mit sich führt.“

Welchen Gefahren sind die Bürgerinnen und Bürger bei der Nutzung des Passes ausgesetzt?

Die angeblich fälschungssicheren Dokumente können nachgemacht, die Identität kopiert werden oder eine Person kann mittels ihres Passes elektronisch verfolgt werden.



Wenn ein Reisepass wirklich benötigt wird, so sollte er grundsätzlich in einer Schutzhülle aus Aluminiumfolie aufbewahrt werden, wodurch das unbemerkte elektronische Auslesen des RFID-Chips verhindert wird.

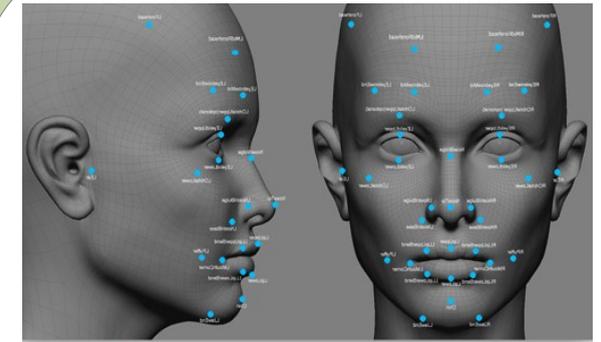
Nochmal zur Klarstellung: Dies ist kein Horrorszenarium sondern ein Auszug aus der offiziellen Broschüre zur Info bei einer Passbeantragung!

Möglicher Missbrauch der biometrischen Daten auf dem RFID-Chip

Welchen Wert haben die Daten auf dem Chip? Neben den „normalen“ Daten zur Person sind nun auch das biometrische Foto und ein Fingerabdruck, künftig mit dem EU-Entry-Exit System alle 10 Fingerabdrücke auf dem Chip und können leicht in fremde Hände geraten.

Damit können Verbrechen mit meiner Identität begangen werden und ich muss meine Unschuld beweisen (Umkehr der Unschuldsvermutung).

Meine biometrische Daten gehören mir, mein Körper, meine Identität wird auf einen Zahlencode reduziert. Geräte, die für medizinische Untersuchungen entwickelt wurden, werden für polizeiliche Kontrollmöglichkeiten missbraucht, ohne dass ich mich dagegen wehren kann/darf. Diese Vermessung ist eine „erkennungsdienstliche Maßnahme“ für die es eigentlich einen Anlass geben müsste.



Über den entwürdigenden Zwang, dass sogar mein Verhalten bestimmt wird (ich darf auf einem biometrischen Foto nicht lächeln) werden meine Persönlichkeitsrechte eingeschränkt, da ich keine Information bekomme, wer über meine Daten verfügen kann.

Hinzu kommen weitere mögliche Missbrauchsmöglichkeiten durch (Geheim-) Dienste derjenigen Staaten, denen man durch seine Einreise die Gelegenheit zum Lesen seiner Daten gegeben hat.

Und nicht vergessen: RFID Chips mit weltweit eindeutigen IDs gibt es inzwischen in vielen Produkten, vor allem Textilien. Wenn man diese nicht sorgfältig nach dem Kauf entfernt, wissen vielleicht andere, wie lange man seine Unterhose schon trägt ...

*... genauso kann man mich durch die alltägliche Videoüberwachung in den Straßen verfolgen, wenn man im Besitz meines biometrischen Fotos ist (siehe unser **Indect-Flyer**).*

Was kann man tun?

Informieren Sie sich über die Gefahren der RFID-Technik und der biometrischen Körpererkennung.

Wehren Sie sich!

Wir alle haben etwas zu verbergen – unsere Privatsphäre!

**Engagieren Sie sich für Ihre Bürgerrechte!
Bürgerrechtsarbeit kostet Geld
Spenden Sie**