


 13th Symposium
on Privacy and Security

Neue Datenschutztechnik für neue Herausforderungen

Marit Hansen
Stellvertretende Landesbeauftragte für Datenschutz
Schleswig-Holstein

Zürich, 9. September 2008
«Informatik und Datenschutz im Widerstreit?»


ULD 
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

ULD  www.datenschutzzentrum.de

Überblick

- Datenschutz vs. Technik?
- Grundbegriffe der Datenschutztechnik
- Heutige und künftige Datenschutztechnik
- Fazit

13th Symposium on Privacy and Security


ULD  www.datenschutzzentrum.de

Informatik-Baumeister

«Unter hoher Wachstumsgeschwindigkeit hat die Informatik kein professionelles Selbstverständnis entwickelt, das per se zuverlässig und bedachte Konstruktionen zum beruflichen Normalfall werden lässt.»

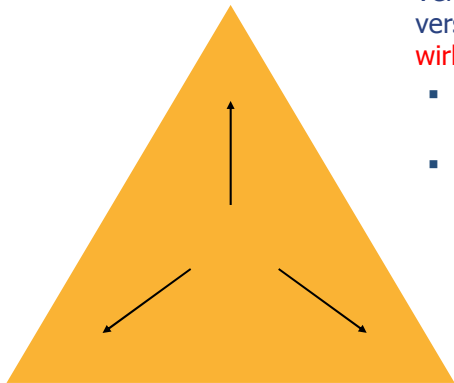
Wolfgang Coy (1992)

13th Symposium on Privacy and Security

ULD  www.datenschutzzentrum.de

**Technik:
Design, Implementierung und Betrieb**

Funktionalität

Daten-sicherheit  **Daten-schutz**

Verschiedenes **Niveau** und verschiedene **Wechselwirkungen**:

- Teilweise wechselseitige Schwächung
- Teilweise ist hohes Niveau in allen Bereichen möglich

13th Symposium on Privacy and Security

 www.datenschutzzentrum.de

Spannungsfeld Technik ↔ Datenschutz

- Technik-Ziel: Vermeidung von Redundanzen (und daraus resultierenden Fehlern) in Datenbanken
- «Natürliche» Lösung: eine weltweite Zentral-Datenbank für alle Informationen zu jeder Person
- Probleme:
 - Begehrlichkeiten von Marketing-Abteilungen, Arbeitgeber, Versicherungen, Kriminellen ...
 - Zentraler Angriffspunkt
 - Zugriffskontrolle
 - Änderungen in einem Bereich: unsichtbar für andere?
 - Einfluss des Betroffenen, wer was über ihn weiß?

13th Symposium on Privacy and Security

 www.datenschutzzentrum.de

Spannungsfeld Technik ↔ Datenschutz

- Technik-Ziel: mehrfach verwendbare Applikationen
- «Natürliche» Lösung: umfassende Digitalisierung, kontextübergreifende Identifikatoren, Interoperabilität und Offenheit für vielseitige Nutzungsmöglichkeiten
- Probleme:
 - Begehrlichkeiten ...
 - Unkontrollierte und unkontrollierbare Verkettbarkeit
 - «Funktion Creep»; Aufweichung einer Zweckbindung
 - Durchsetzbarkeit von Löschen und Sperren?

13th Symposium on Privacy and Security

ULD  www.datenschutzzentrum.de

Leitbildwechsel

*«So wie es bisher schon einen auf Gesetze und Konventionen gegründeten und organisatorisch implementierten **Schutz von personenbezogenen oder sicherheitssensiblen Daten** gab, so lässt sich dieser Schutz **auch technisch realisieren**, sogar ohne dass es dazu übergeordneter Einflussnahme bedürfte.»*

Günter R. Koch und John Favaro (1984)


13th Symposium on Privacy and Security

ULD  www.datenschutzzentrum.de



**Grundbegriffe
datenschutz-
fördernder
Technik**

13th Symposium on Privacy and Security

ULD  www.datenschutzzentrum.de

Was sind Privacy Enhancing Technologies?

**«Privacy Enhancing Technologies (PET)
are a coherent system of ICT measures
that protects privacy [...]
by eliminating or reducing personal data or
by preventing unnecessary and/or
undesired processing of personal data;
all without losing the functionality
of the data system.»**

Borking / Raab (2001)

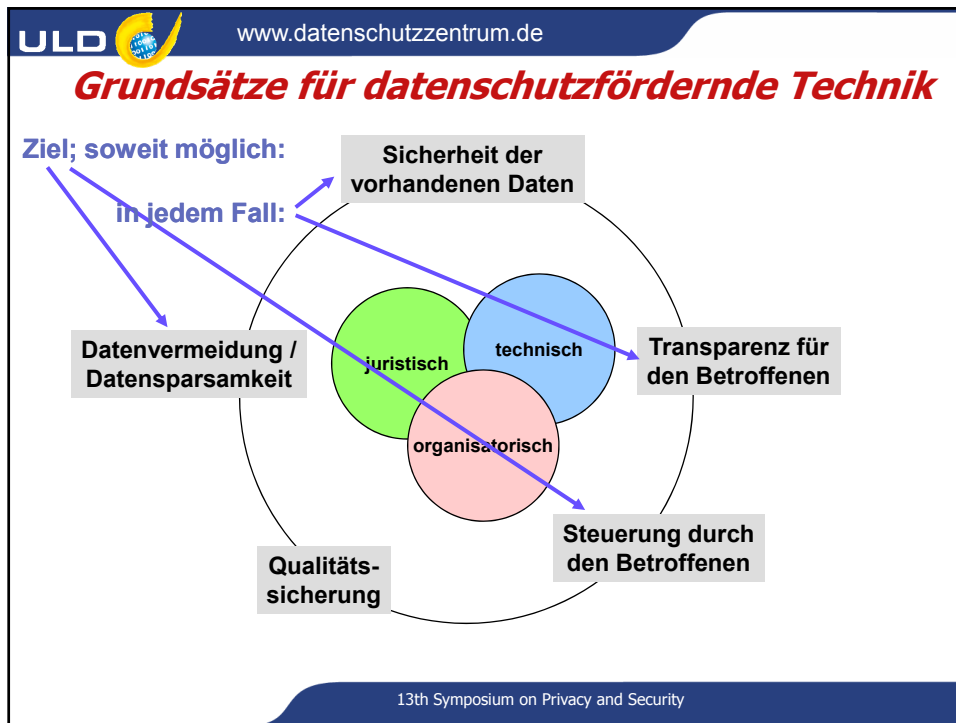
13th Symposium on Privacy and Security


ULD  www.datenschutzzentrum.de

Datenschutzfreundliche Techniken

- D.h. datenschutzgerechte und datenschutzfördernde Technik
- Begriffe:
 - **Privacy Enhancing Technologies (PET):**
datenschutzfördernde Technik
 - **Systemdatenschutz:**
Datenschutz eingebaut in Technik und Verfahren
 - **Selbstdatenschutz:**
Steuerung/Kontrolle durch den Nutzer über seinen Datenschutz
 - **Mehrseitige Sicherheit:**
Alle Parteien formulieren ihre Schutzziele
und setzen sie (gem. *Aushandlungsergebnis*) durch

13th Symposium on Privacy and Security




www.datenschutzzentrum.de

1) *Datensparsamkeit*

- Für personenbezogene Daten **minimieren**:
 - Erfassungsmöglichkeit
 - Erfassung
 - Verwendungsmöglichkeit
 - Verwendung
- **Datensparsamkeit** \approx **Erforderlichkeit + Zweckbindung**
auch für die Gestaltung technischer Systeme
- **Datenvermeidung**: maximale Datensparsamkeit
- Verfahren zu **Anonymität** und **Pseudonymität**
zur Nutzung und Bezahlung von Diensten

13th Symposium on Privacy and Security


www.datenschutzzentrum.de


«*Privacy-Modus*» im Browser



Datensparsamkeit im Browser:

- Kein Eintrag in History, Formular- und Passwortspeicher
- Keine Speicherung von URLs und Suchanfragen
- Löschen der temporären Daten
- Verbessertes Cookie-Management


13th Symposium on Privacy and Security

ULD  www.datenschutzzentrum.de


Cookie-Management mal anders: CookieCooker

- Nutzer tauschen Cookies untereinander aus
- Resultat: verwischte Profile per Cookies

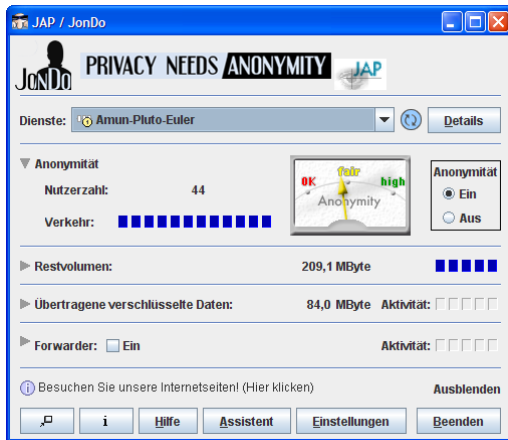
⇒ Nicht unbedingt datensparsam!



13th Symposium on Privacy and Security


ULD  www.datenschutzzentrum.de

«Anonymizer»

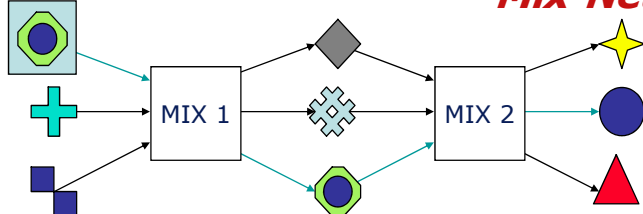


- Anonymisierer, z.B. AN.ON auf Ebene der IP-Adressen
- Eine technische Anonymitätsmethode: «Gleichmacherei»
- Steigerung: Unbeobachtbarkeit

13th Symposium on Privacy and Security

ULD  www.datenschutzzentrum.de

Mix-Netz (Chaum 1981)



- **Grundidee:**
 - Nachrichten in einem «Schub» sammeln, umkodieren, umsortieren, gemeinsam ausgeben
 - Alle Nachrichten haben dieselbe Länge
 - Mehr als einen Mix verwenden
 - Wenigstens ein Mix darf nicht angreifen
- **Ziel:**
 - **Unverkettbarkeit** von Sender und Empfänger

13th Symposium on Privacy and Security

ULD  www.datenschutzzentrum.de


Unverkettbare Berechtigungsnachweise (Chaum 1984 ff.)

- Private Credentials
- Anderer Name: Minimal Disclosure Tokens
- Einsatzbereiche:
 - TPM (Trusted Platform Module) 1.2
 - PRIME – Privacy and Identity Management for Europe
 - Zukünftig:
 - Microsoft CardSpace?
 - eGov-Projekte?
- **Ziel:**

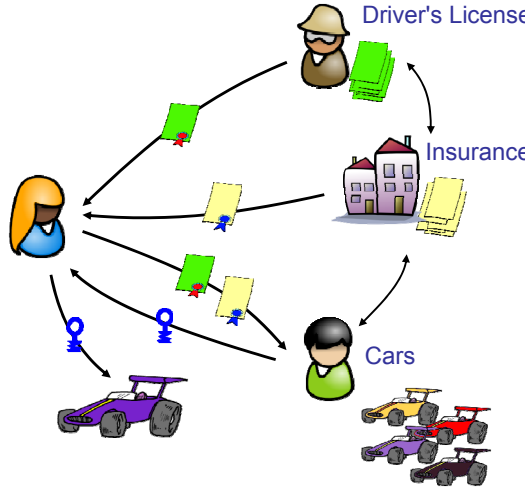
Kombination von Anonymität und starker Authentisierung



13th Symposium on Privacy and Security

ULD  www.datenschutzzentrum.de


Normalfall: Verkettbare Informationen



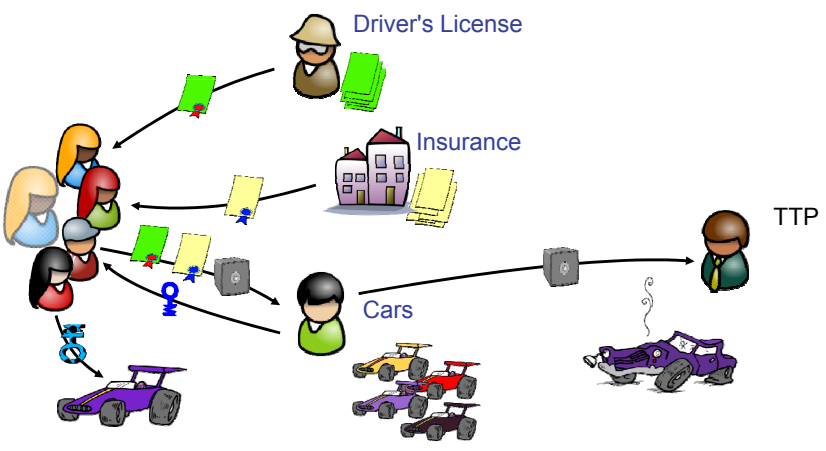
The diagram illustrates a network of interconnected entities. At the top is 'Driver's License' (represented by a person with a hat and a stack of green documents). Below it is 'Insurance' (represented by a house and a stack of yellow documents). At the bottom is 'Cars' (represented by a person and several colorful toy cars). Arrows indicate bidirectional relationships: Driver's License ↔ Insurance, Insurance ↔ Cars, and Driver's License ↔ Cars. Additionally, there are arrows pointing from each of these three entities to a central female figure on the left, representing a user. Small icons of documents with red and blue stars are placed along the arrows, suggesting data points or identifiers.

Folie von Jan Camenisch
IBM Research Zürich

13th Symposium on Privacy and Security

ULD  www.datenschutzzentrum.de

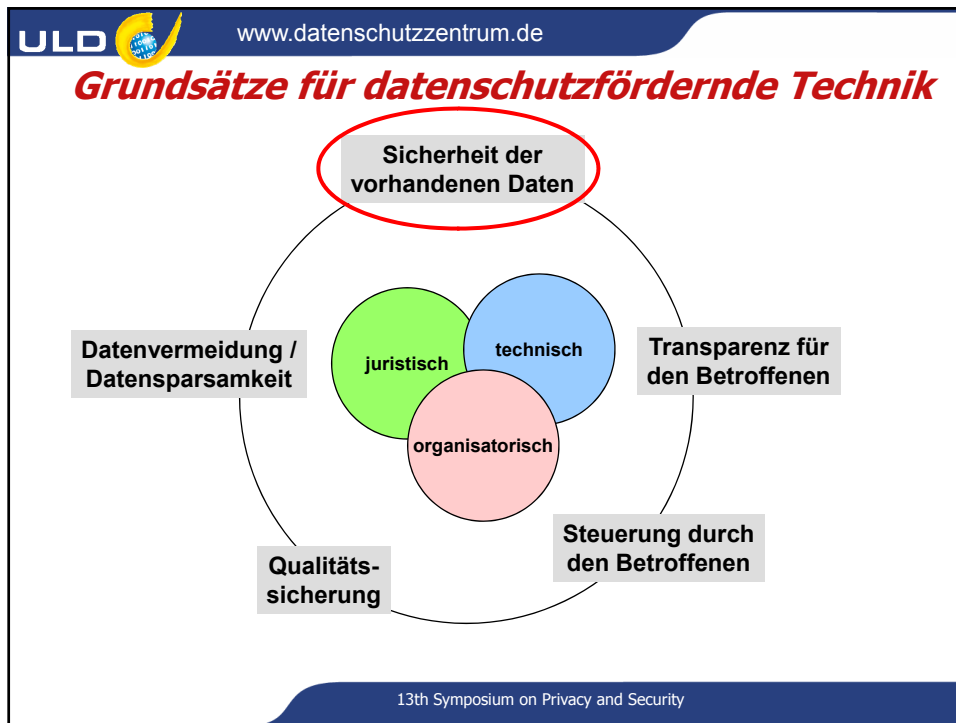
Datensparsamkeit durch Private Credentials




This diagram shows a similar setup to the first slide but with a focus on privacy. It includes 'Driver's License', 'Insurance', and 'Cars' entities. A 'Trusted Third Party' (TTP), represented by a person in a suit, is introduced on the right. A grey box representing a private credential is shown being sent from the 'Cars' entity to the TTP. On the left, a group of diverse people (including a woman, a man, and a child) are shown. Arrows indicate that these individuals receive information from the 'Driver's License', 'Insurance', and 'Cars' entities. The private credential from the TTP is also directed towards this group, suggesting that the user's data is now more fragmented and less directly linked to the original entities.

Folie von Jan Camenisch
IBM Research Zürich








13th Symposium on Privacy and Security




ULD  www.datenschutzzentrum.de

2) Sicherheit der vorhandenen Daten

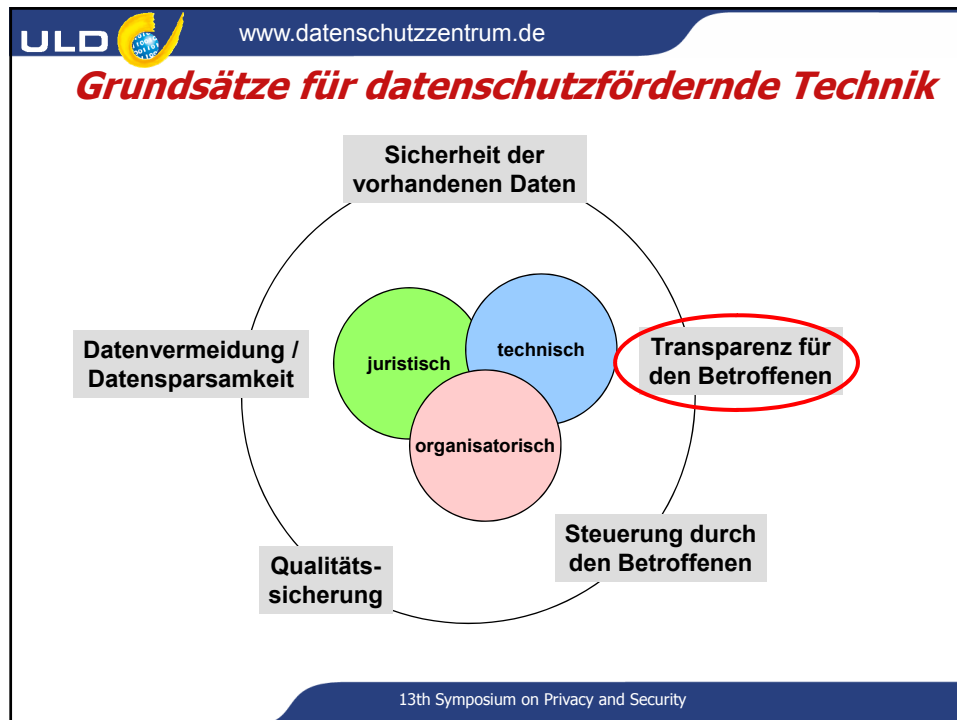
Mindestanzahl Mitwirkender:

-  • Systeme mit feingranularen Zugriffsberechtigungen
-  • manipulations sichere Geräte
-  • Kryptographie
 - Verschlüsselung
 - für Dateien auf Medien
 - für Kommunikation in offenen Netzen
-  • (Verbindliche) digitale Signatur 
-  • Bedienoberflächen
-  • Interaktionskomponenten (z.B. Aushandlung)




```
-----BEGIN PGP-----
0IxWZHhKYoECwCBeIweKU+0Ed
m068SB4ADeGGctd+eacjDT5Ig
TdwAyp18+WOFYxTVEXbqOqjoW
mY4T9zuoSC5e
=lu9g
-----END PGP-----
```

13th Symposium on Privacy and Security



- ULD  www.datenschutzzentrum.de
- ### *3) Transparenz für den Betroffenen*
- Ziel:
 - **Bewusstsein** des Betroffenen über Verarbeitung seiner Daten
 - Transparenz ...
 - ... der **Intention** der Verarbeitung: Privacy Policies
 - ... der **tatsächlichen Datenverarbeitung**:
 - Dokumentation und Unterrichtung
 - Offenlegung von Quellcode / Verfahren
 - Evaluation, Zertifizierung, Gütesiegel
- 13th Symposium on Privacy and Security

ULD  www.datenschutzzentrum.de

Data Track Here you can see who knows your data and get assistance with data correction or removal

Search (Search on personal data, receiver, transactions etc.)

Who have received information about my ?

What data about me has received?

Who have received from me?

Display Info About

Personal data

Receiver

Preference type

Transaction (=Record)

Pseudonyms

Proofs ("Credentials")

Title

Sex

Name

Birthdate

Street

Postcode

City

Country

Email

Tel

Mobile

Fax

Credit card

Bankaccount

Your search returned 10 records

Record Slider Default order Chronological list Alphabetical list by receipt Selected records

Include transactional pseudonyms even if no data have been sent

Amazon 2006-01-15 amazon.co John Primeur john@kau.se Male	Acer 2006-01-16 acer.com John Primeur john@kau.se Male	Dell 2006-01-20 dell.com John Primeur john@kau.se Male	Mozilla Store 2006-01-25 mozilla.com John Primeur john@kau.se Male
---	--	--	--

2006-01-01 < > 2006-01-27

**Beispiel
«Data
Track» in
PRIME:
Trans-
aktions-
protokoll
beim
Nutzer**

ULD  www.datenschutzzentrum.de

Security Breach Notification

- Verpflichtung in vielen US-Staaten
- Geplant für EU in einigen Sektoren
- Ziel: Information der Betroffenen über Sicherheitsvorfälle



That's not something you want to tell your customers. Which is why you should care about legislation that determines when you have to.

13th Symposium on Privacy and Security

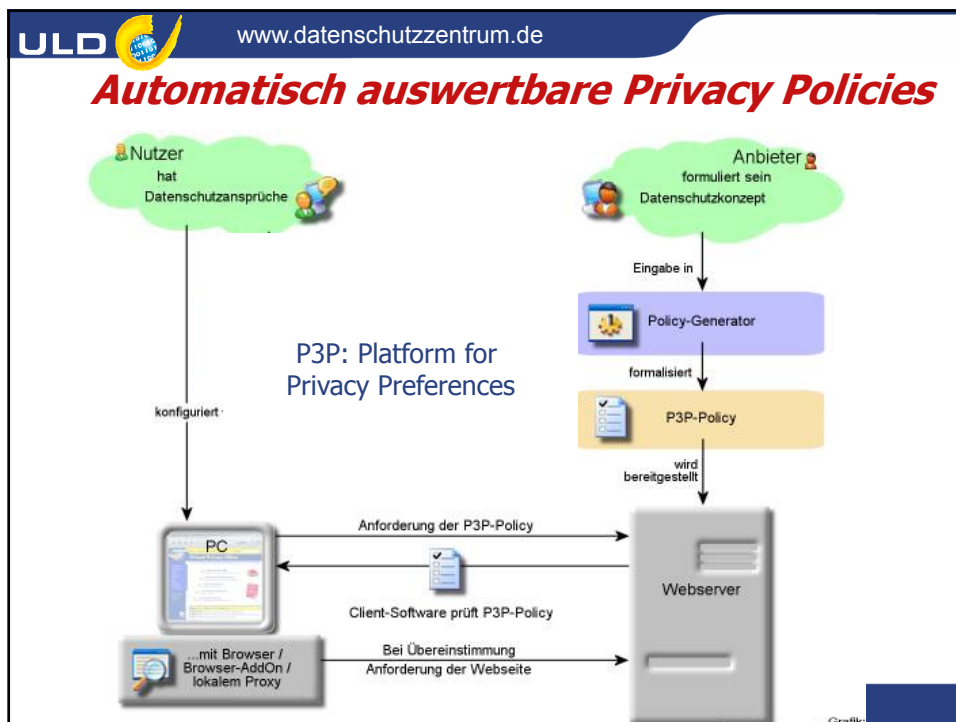
ULD  www.datenschutzzentrum.de

Beispiel: Security Feed in PRIME

- Information über Sicherheits- & Datenschutzvorfälle und Bedrohungen
- Implementiert als RSS-Feed
- Sofern standardisiert: auswertbar von Applikationen



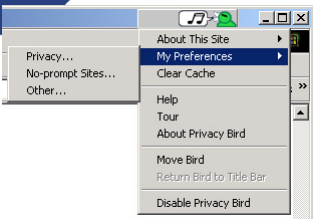

13th Symposium on Privacy and Security



www.datenschutzzentrum.de

Beispiel: Privacy Bird (Lorrie Cranor et al.)

- Der «Privacy Bird» prüft P3P-Policies.
- Information des Nutzers über Aussehen und Sound des Vogels

13th Sympos

The singing **green bird** appears when Privacy Bird determines that a web site's privacy policy matches your preferences. If the site contains images or other embedded content that do not have privacy policies associated with them, or that have privacy policies that do not match your preferences, a red exclamation point will appear next to the notes in the bird's song bubble.








The angry **red bird** appears when Privacy Bird determines that a web site's privacy policy conflicts with your preferences.

The uncertain **yellow bird** appears when Privacy Bird is unable to fetch or read a privacy policy from the web site you are visiting. The policy must be encoded according to the Platform for Privacy Preferences (P3P) standard in order for the Privacy Tool to fetch it. If the policy contains an error or if it has expired or is not valid, the yellow bird will appear. While a web page is loading and Privacy Bird is in the process of looking for the accompanying privacy policy, the yellow bird will appear to be turning its head from side to side.


The sleeping **gray bird** appears when Privacy Bird has been disabled.

ULD www.datenschutzzentrum.de

Beispiel: Privacy Policy Icons (Mary Rundle 2006)

	You agree not to use this data for marketing purposes.
	You agree not to trade or sell this data.
	You agree to submit to a third-party audit program on data use; if government has requested access to my data, you agree to involve my governmental ombudsman.
	You agree to make available to me the data that you have on me without my having to pay for it/at a minimal charge.
	You allow me to address inaccuracies in the data and request its removal.
	You agree to take reasonable steps to keep my data secure.
	You agree to arrange with X organization to help resolve any disputes we have over your treatment of this data. [The seal / name of the entity follows.]































13th Symposium on Privacy and Security

ULD  www.datenschutzzentrum.de


Iconset for Data-Privacy Declarations v0.1


Beispiel: Icons (Mehldau 2007)

Let's simple declare what data is how used, stored, given away or deleted.

What data?	How is my Data handled?	For what purpose?	For how long?
 Username / Real Name	 deleted	 Statistics	 end of usage / logout
 Real Name / Adress	 saved	 Advertisement	 end of contract
 IP, Files, Time	 anonymized	 Shopping	 timestamp / hours
 Mailadress	 encrypted		 days
 Comments, Conversations	 published		 weeks
 Mails, Messages	 passed on		 month
 Contacts, Friends	 for friends of friends		 years
 Favourites, Interests	 for Friends, Contacts		 for the time being
 Edits	 if you choose		
 Cookies			














Iconset „Data-Privacy Icons v0.1“ by Matthias Mehldau wetter@berlin.ccc.de
Font „Yanone Kalfesatz“ by Jan Gerner http://www.yanone.de/
both licensed under Creative Commons Namensnennung 2.0 Deutschland http://creativecommons.org/licenses/by/2.0/de/




ULD  www.datenschutzzentrum.de

Iconset for Data-Privacy Declarations v0.1

Let's simple declare what data is how used, stored, given away or de

What data?	How is my Data handled?	For what purpose?
 Username / Real Name	 deleted	 Statistics
 Real Name / Adress	 saved	 Advertisement
 IP, Files, Time	 anonymized	 Shopping
 Mailadress	 encrypted	
 Comments, Conversations	 published	

Iconset „Data-Privacy Icons v0.1“ by Matthias Mehldau wetter@berlin.ccc.de
Font „Yanone Kalfesatz“ by Jan Gerner http://www.yanone.de/
both licensed under Creative Commons Namensnennung 2.0 Deutschland http://creativecommons.org/licenses/by/2.0/de/



ULD  www.datenschutzzentrum.de

Auswertung von White Lists und Black Lists

- Nutzer muss selbst Filter seines Vertrauens vorgeben

Schwarze Liste einer schwedischen Verbraucherschutz-Organisation:

Datenschutz-Gütesiegel in Abwandlung für White Lists denkbar:




7 Augusti 2007
www.radron.se

Till startsidan

Testor
Svarta listan
Märkningar
Klagoguide
Råd & Rön bilagor
Länkar

Beställ
Om Råd & Rön
Nästa nummer
Om cookies
Vanliga frågor
Kontakta oss

PRENUMERERA

GE BORT EN PRENUMERATION

Senaste numret Sök

Logga in: Prenumeranter | 24 timmar

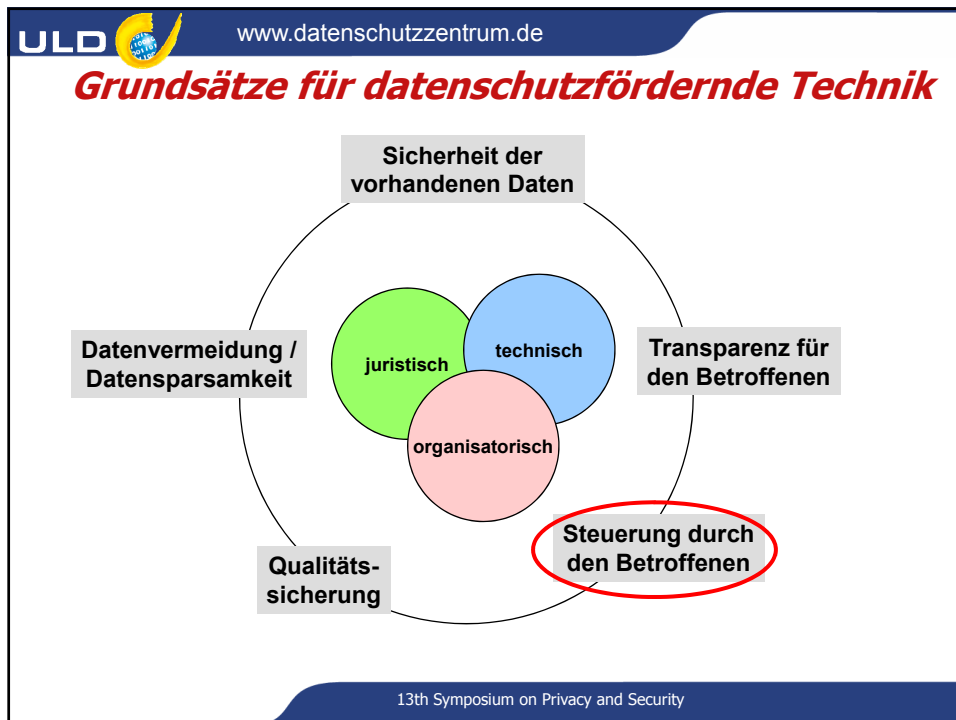
Svarta listan


Ny sökning

Sökträffar:

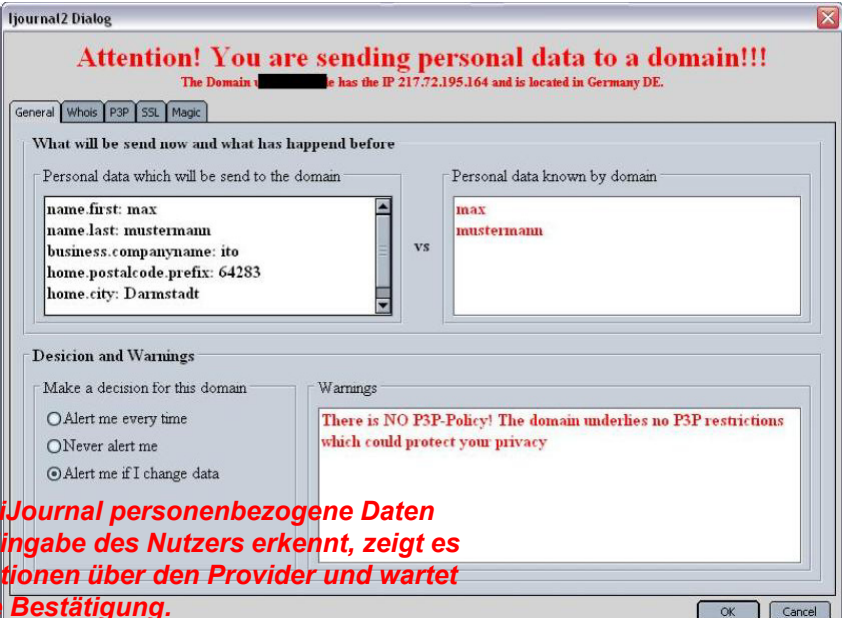
Motor: AB Kurt Ålund Bilaffär i Lidingö, Lidingö,
Resor: Adriatic Buss AB, Norrköping, Företaget har upphört.
Bostad: AII Partner AB, Stockholm, Antal ärenden: 2.
Resor: Air France, Stockholm, Delvis rättelse.
Motor: Ailt i Däck o Fälg i Åled, Åled,
Flytt, sport, optik, frisör m
Resor: Almedals Flyttexpress, Malmö, Ärendet har gått vidare till tingsrätt.
Motor: Amazonas Travel, Stockholm,
Resor: Anna's Bil & Maskin Försäljning Kommanditbolag, Nyhamnsläge,
Företaget har upphört.
Motor: Annelövs Husbilimport AB, Luddköpinge, Företaget har upphört.
Bostad: Autohaus, Helsingborg, Ärendet har gått vidare till tingsrätt: Parterna
förlikades i tingsrätt. Företaget har tidigare förekommit på Råd & Rön's svarta
lista.
Motor: Autopoint i Lund AB, Lund, Ärendet har gått vidare till tingsrätt.
Motor: Autos i Örebro, Örebro,
Motor: Autotrading i Luleå AB, Gammelstad,
Bostad: Badrumsbutiken, Täby ,
Resor: Benny Toftling, Fellingsbro,
Resor: Bentour International AB, Stockholm, Ånge, Företaget har upphört.
Motor: Antal ärenden: 5.
Motor: Bergsviks Sko- och Nyckelservice, Karlstad,

13th Symposium on Privacy and Security




ULD  www.datenschutzzentrum.de


Beispiel: iJournal (Plug-in für Mozilla)



Sobald iJournal personenbezogene Daten in der Eingabe des Nutzers erkennt, zeigt es Informationen über den Provider und wartet auf eine Bestätigung.

atus  www.datenschutzzentrum.de

Beispiel: «A Toolkit for Usable Security Freiburg»



Die rot markierten Daten werden jedoch von der aktuellen Identität geschützt.

13th Symposium on Privacy and Security

ULD  www.datenschutzzentrum.de

4) Steuerung durch den Betroffenen


im Vorfeld: Steuerung

- ... der Hergabe eigener Daten:
 - Bestimmung des Personenbezugs (Pseudonymität, Datenumfang)
 - Formulierung
 - Aushandlung
- ... der Anforderungen an die Verwendung:
 - Bedingungen wie Zweck, Dauer, Gegenleistung

während / nach Verwendung:

- Technikunterstützung bei:
 - Einwilligung
 - Widerspruch
 - Auskunft
 - Berichtigung
 - Löschen
- Nachprüfbarkeit:
 - «Einzelnutzungsnachweis»
 - Abfragbares Logfile
 - Eigene Protokollierung

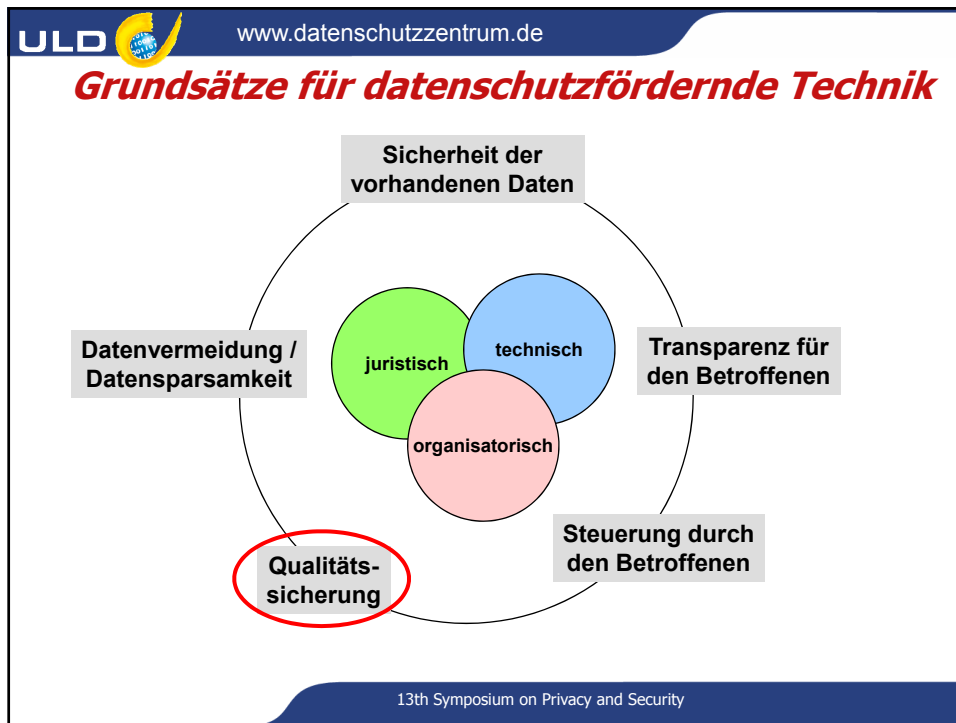
13th Symposium on Privacy and Security

ULD  www.datenschutzzentrum.de

Rechtewahrnehmung unterstützen: Angebot der Online-Auskunft

Simulations Assistance Help

Data Track Here you can see who knows your data and get assistance with data correction or removal



ULD  www.datenschutzzentrum.de

Aktuelles Beispiel: Viren in einer NASA-Raumstation

Virus Infects Space Station Laptops (Again) | Threat Level from Wired.com - Mozilla Firefox

Virus Infects Space Station Laptops (Again)

By Ryan Singel August 26, 2008 | 2:22:55 PM Categories: Hacks

...

"This is not the first time we have had a worm or a virus," NASA spokesman Kelly Humphries said. "It's not a frequent occurrence, but this isn't the first time."

...

NASA declined to name the virus, but SpaceRef.com, which broke the story, reported that the worm was *W32.Gammima.AG* worm -- a worm first detected in August 2007 that installs software that steals credentials for online games.

...

"Everything is scanned before it goes up, so it's an indirect connection," Humphries said.

AS for whether mission critical systems are connected to the same network as these kinds of laptops?

"I don't know and even if I did, I wouldn't be able to tell you for IT security reasons," Humphries said.




www.datenschutzzentrum.de


5) Qualitätssicherung

In der Vergangenheit rein organisatorisch verstanden, aber Technik kann hier unterstützen:

- Protokollierung
- Implementieren von «Prüfpunkten» für interne / externe DSBs
- Policy-Enforcement



13th Symposium on Privacy and Security


www.datenschutzzentrum.de

Sticky Policies

- Policy wird an Daten «geklebt» und ausgewertet
- Für Policy: standardisierte Datenschutzmanagementsprache

Actual data stored in the data repository

Privacy Policy

“Control”

Encrypted Personal Data

Encrypted with TPS Public Key:

- Symmetric key used to encrypt personal data
- Hash of privacy policy

TPS: Trusted Privacy Service

Folie von Marco Casassa Mont
Hewlett-Packard Lab Bristol


ULD  www.datenschutzzentrum.de

Datenschutzrecht-Implementieren ist nicht leicht ...

Art. 8 EU Directive: The processing of special categories of data

- (1) Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.
- (2) Paragraph 1 shall not apply where:
 - a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or
 - b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
 - c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
 - d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or
 - e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.
- (3) ...


13th Symposium on Privacy and Security

ULD  www.datenschutzzentrum.de



Fazit

13th Symposium on Privacy and Security

ULD  www.datenschutzzentrum.de

Fazit (1/2)

Datenschutz und Datenschutztechnik ...

- ... sind Teil diverser Spannungsfelder, z.B. in Bezug auf
 - «naive» Informatikkonzepte und -implementierungen,
 - Bequemlichkeit, Unwissenheit und Unmündigkeit,
 - datenschutzfeindliche Business-Modelle,
 - innere Sicherheit.
- ... wirken aufgepfropft schlechter als integriert, besonders was Infrastrukturen betrifft.
- ... sind heutzutage zu komplex.

13th Symposium on Privacy and Security

ULD  www.datenschutzzentrum.de

Fazit (2/2)

Datenschutztechniken ...

- ... sind im «Labor» schon weit konzipiert. Der massenhafte Einsatz fehlt aber.
- ... profitieren von Anreizen für besseren Datenschutz und Sanktionen für einen schlechten.
- ... sind in ihren Wechselwirkungen noch unerforscht.

⇒ **Trend zu stärker ausgereifter, einfacher bedienbarer und besser integrierter Datenschutztechnik**




13th Symposium on Privacy and Security

ULD  www.datenschutzzentrum.de

Vielen Dank für Ihre Aufmerksamkeit!

13th Symposium on Privacy and Security