Datenschutz ohne DSGVO

Dirk Ihnen

49 Jahre alt
Physiker
IT-Sicherheitsbeauftragter (TÜV)
IT-Organisation der Ev. Luth. Kirche in OL

Gesetze schützen Daten nicht

- Gesetz ist nur Text
- Gesetz kann nix tun
- Gibt nur Strafen vor wenn …
- Eigentlich nutzlos?

- Daher ohne DSGVO

Datenschutz u. IT-Sicherheit

- Personen bezogenen Daten

- Verfügbarkeit, Vertraulichkeit, Integrität

Gefahren?

Tapfer du sein musst!

Meister welche Gefahren drohen mir ?

Was war das denn?


Stiftung
Datentest
datenschutz
Datenschutz:
Mangelhaft
(5,2)
Im Test:
42 Datenkraken
Ausgabe 01/2017
digitalcourage.de
17DC-BI

Gefahren

- Das eigene Foto in der Verbrecherkartei
- Kreditwürdigkeit
- Nachteile in persönlicher Entfaltung
- Privatsphäre
- ...

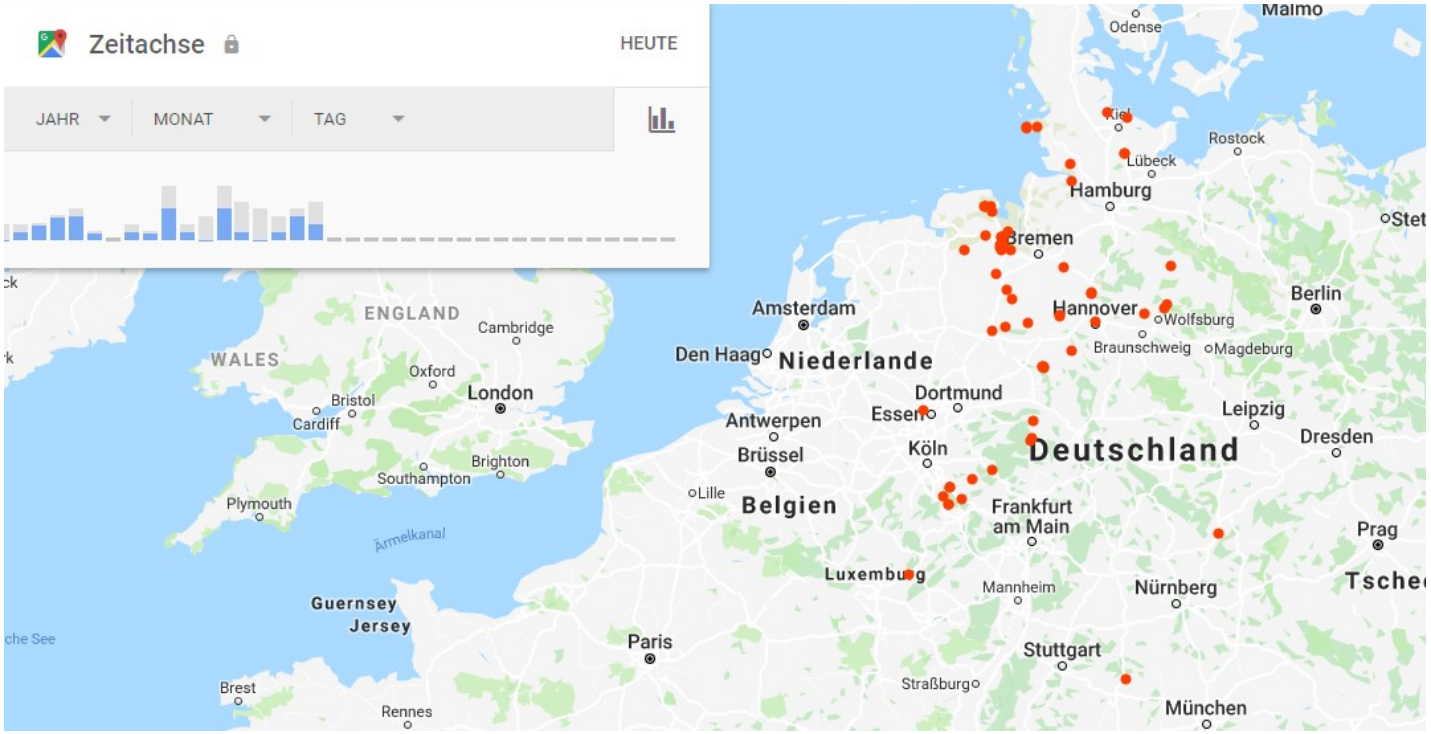
Wo sind die Daten

- Datenbanken
- Dateien
- ...

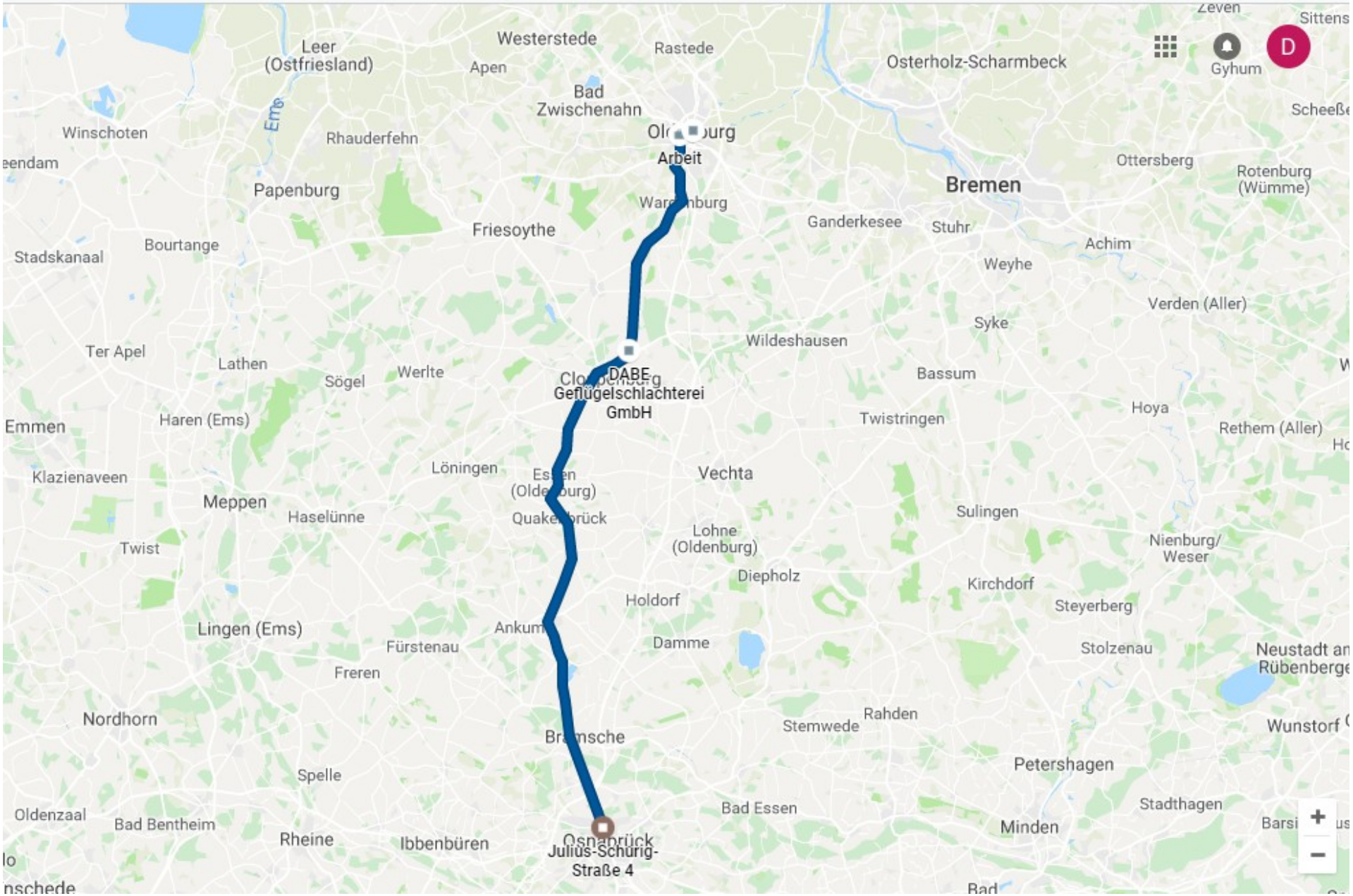
- Nur ein Mausklick entfernt

Schaust du hier:

- https://adssettings.google.com/authenticated?hl=de
- https://www.google.com/maps/timeline?pb
-



Ziemlich genau!



Wer bin ich?

- https://myactivity.google.com/myactivity

  meine Suchanfragen

- https://myaccount.google.com/permissions?pli=1

  meine Geräte

Facebook

- Wer sich wahrscheinlich politisch betätigt
- Konservative und Liberale
- wer ein Motorrad besitzt
- … u.v.m.

- https://netzpolitik.org/2016/98-daten-die-facebook-ueber-dich-weiss-und-nutzt-um-werbung-auf-dich-zuzuschneiden/

Digitale Selbstverteidigung

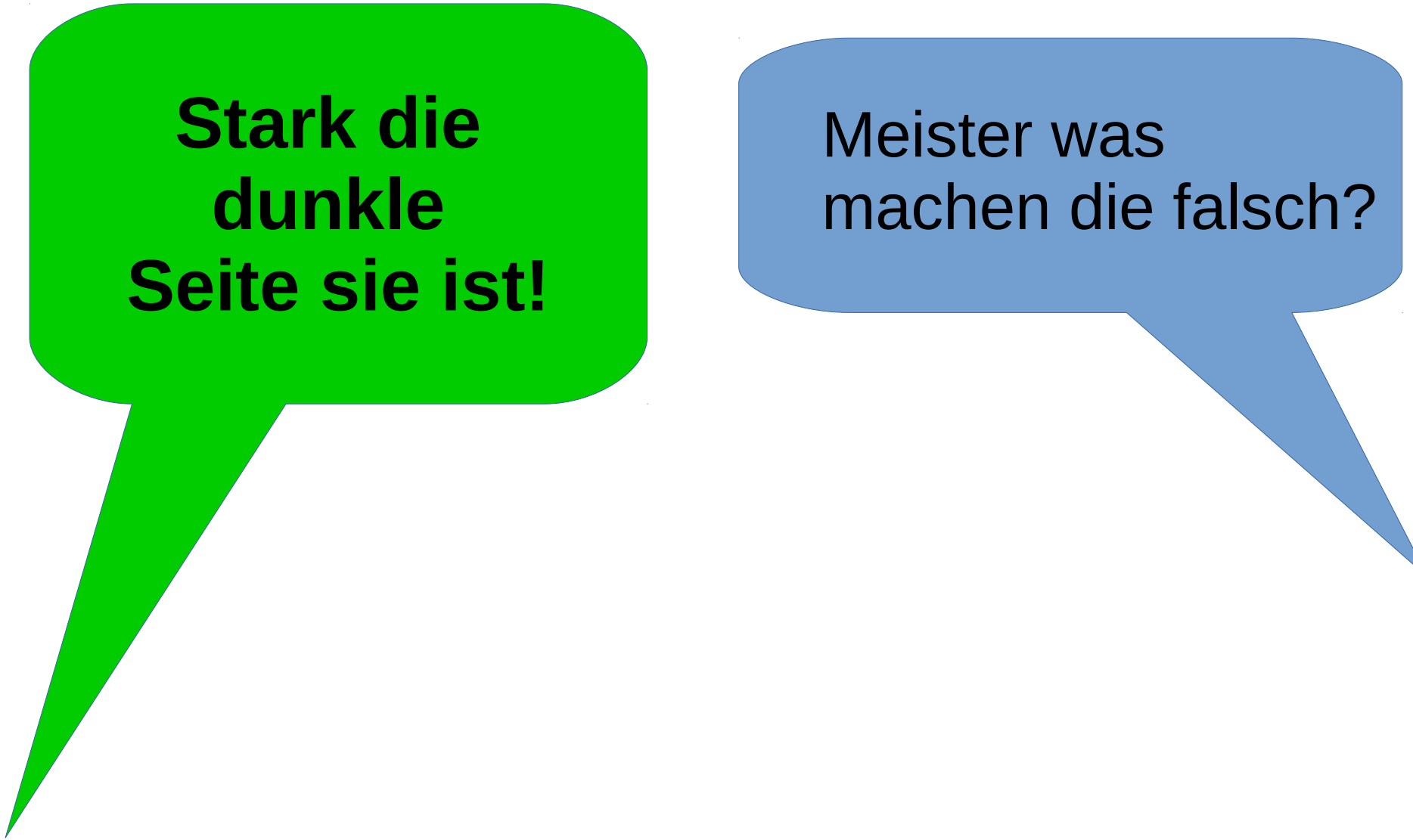
- Datenschutz ernst nehmen

- Darauf achten Daten zu schützen
  - Verschlüsseln, Anonymisieren
  - Abgreifen verhindern
  - Verstöße anprangern
  - Informieren!
  - ...

Nicht auffallen?

- Best. Dienste nicht nutzen
- Keine reale Informationen preisgeben
- …

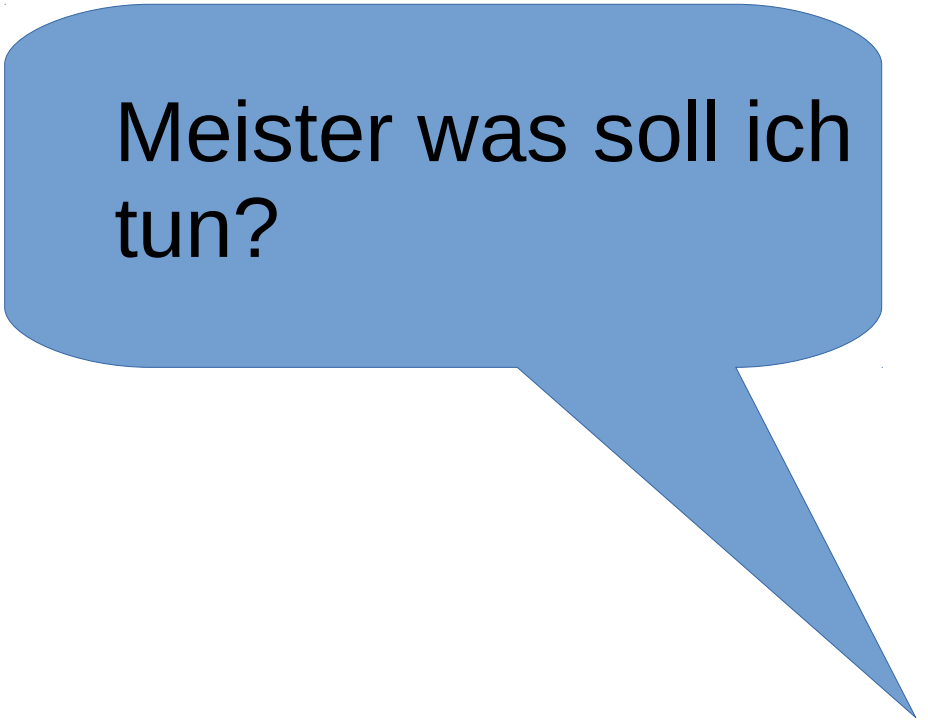
- Fast nicht machbar


Stark die dunkle Seite sie ist!
Meister was machen die falsch?

Probleme beim Eigenschutz

- Dummheit
- Ignoranz
- Schlamperei
- Geiz
- Gier
- **Faulheit**


Helfen den Schwachen du musst!


Meister was soll ich tun?

Be water my friend!

Digitales Karate

1. DAN den Gegner erkennen

Für APPs gilt:

- Grund der Datenerfassung, -speicherung und/ oder –verarbeitung
- Art der durch die App erfassten Daten (Metadaten, Inhaltsdaten, personenbezogene Daten)
- Dauer der Speicherung
- Nennung von zugriffsberechtigten Dritten
- Belehrung zwecks Auskunftsrecht, Widerruf und Löschung der Daten
- Nennung der verantwortlichen Stelle, inklusive Kontaktmöglichkeit

Sieht in der Praxis so aus:

- b) Für den Fall, dass die IBM bei einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit dem Betrieb der eGA gesetzlich verpflichtet sein sollte, durch diese Verletzung betroffene Nutzer der eGA unverzüglich zu informieren, stellt die TK der IBM - sofern Sie als Nutzer betroffen sind - Ihre gegenüber der TK angegebene Mobiltelefonnummer der IBM unverzüglich zur Verfügung. Sollte Ihre Mobiltelefonnummer bei der TK nicht hinterlegt sein, stellt die TK Ihre gegenüber der TK angegebene E-Mailadresse zur Verfügung.

- https://www.tk.de/techniker/unternehmensseiten/unternehmen/die-tk-app/tk-app-datenschutz-2023688

Digitales Karate

2. DAN festen Stand behalten

Privacy by default

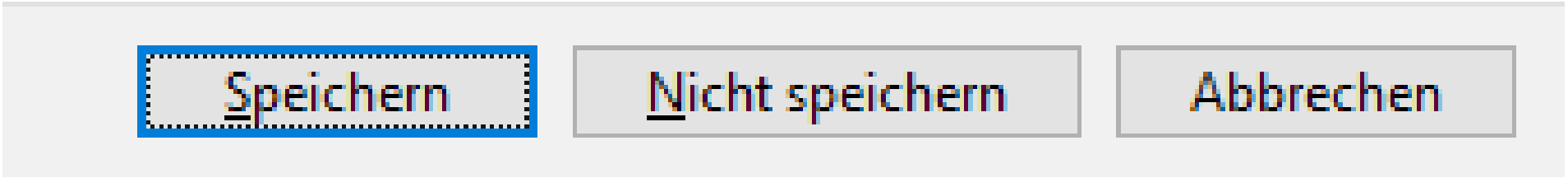
Preisgeben von Daten

- Nicht durch Installieren sondern
- Bewusst durch den User selber gemachte Aktionen

Datenschutz!

Hallo UserIn,

Du willst wirklich deine
privaten Daten
für die Zentrale des FBI, des BND und
der Aroganz Versicherung
dauerhaft freigeben?

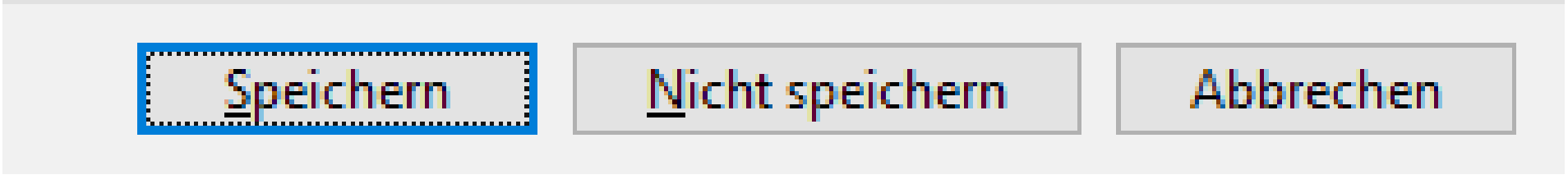


Achtung Selbstschutz !

Hallo UserIn,

Du willst wirklich deine
privaten Daten
für die Zentrale des FBI, des BND und
der Aroganz Versicherung
dauerhaft freigeben?

Wenn du nicht sicher bist klicke Hier



Privacy by Design

Digitale Selbstverteidigung

- Datenschutz ernst nehmen

- Darauf achten Daten zu schützen
  - Verschlüsseln, Anonymisieren
  - Abgreifen verhindern
  - Verstöße anprangern
  - Informieren!
  - ...

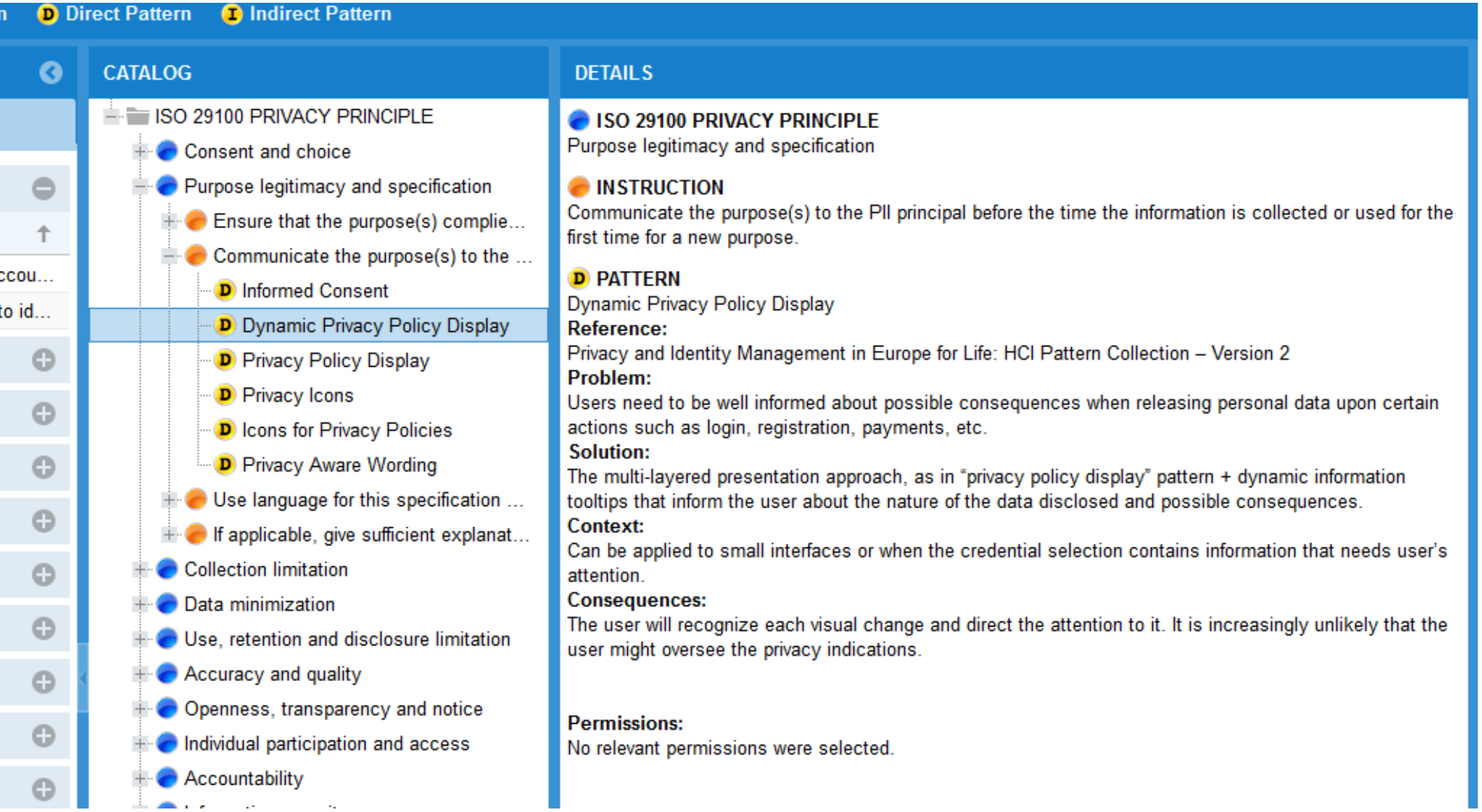
Privacy by Design

- Datenschutz ernst nehmen

- Darauf achten Daten zu schützen
  - Verschlüsseln, Anonymisieren
  - Abgreifen verhindern
  - Verstöße anprangern
  - Informieren!
  - ...

Keine Musterlösungen

- Designvorgaben (Joel test 7)
- Tests von Anfang an! (Joel test 12)
- Privacy Pattern
  http://privacypatterns.wu.ac.at:8080/catalog/


Direct Pattern
Indirect Pattern
CATALOG
ISO 29100 PRIVACY PRINCIPLE
Consent and choice
Purpose legitimacy and specification
Ensure that the purpose(s) complie...
Communicate the purpose(s) to the ...
Informed Consent
Dynamic Privacy Policy Display
Privacy Policy Display
Privacy Icons
Icons for Privacy Policies
Privacy Aware Wording
Use language for this specification ...
If applicable, give sufficient explanat...
Collection limitation
Data minimization
Use, retention and disclosure limitation
Accuracy and quality
Openness, transparency and notice
Individual participation and access
Accountability
DETAILS
ISO 29100 PRIVACY PRINCIPLE
Purpose legitimacy and specification
INSTRUCTION
Communicate the purpose(s) to the PII principal before the time the information is collected or used for the first time for a new purpose.
PATTERN
Dynamic Privacy Policy Display
Reference:
Privacy and Identity Management in Europe for Life: HCI Pattern Collection – Version 2
Problem:
Users need to be well informed about possible consequences when releasing personal data upon certain actions such as login, registration, payments, etc.
Solution:
The multi-layered presentation approach, as in "privacy policy display" pattern + dynamic information tooltips that inform the user about the nature of the data disclosed and possible consequences.
Context:
Can be applied to small interfaces or when the credential selection contains information that needs user's attention.
Consequences:
The user will recognize each visual change and direct the attention to it. It is increasingly unlikely that the user might oversee the privacy indications.
Permissions:
No relevant permissions were selected.

DETAILS

ISO 29100 PRIVACY PRINCIPLE

Data minimization

INSTRUCTION

Minimize the PII which is processed.

PATTERN

Dynamic Location Granularity

Reference:

Problem:

Personal data aren't (sometimes) processed at the highest level of aggregation.

Solution:

Adapt accuracy of the reported location.

Context:

Location based services.

Consequences:

Ensuring that a reasonable number of users are at the same reported location.

Permissions:

No relevant permissions were selected.

PbD kompakt

- Datenvermeidung
- Kontrollierbarkeit und Transparenz
- Vertraulichkeit der Daten
- Datenqualität
- Möglichkeit der Trennung

skizziert von Peter Schaar, in der Fachzeitschrift „Identity in the Information Society“

Digitales Karate

3. DAN Zurückschlagen u. Niederringen

T-online, reichelt, Amazon, Netflix, Tschibo, Nettokom, BOL, Web, Sygate, Franzis, DKB, Deutsch Bank, Elster, 1und1, Rewe, QNAP, open HPI, Teamdrive, DNSHome, pollin, Simyo, Microsoft, gmx, BHW, Opel, Onstar, Synology, Udemy, coursea,comdirect, Esso,Fujitsu, HP, one, Conrad, Oracle, ARAL, PayBack, SEROM, Villagecon, CeBit, Interboot, Uni-Oldenburg, … u.v.m.

Die DASU APP

- Wann hatte ich Kontakt mit wem
- Welche Daten preisgegeben
- ...
- Jährliche automatische Mail zum Datenabgleich
- Abmahnungsgenerator
- ...

- Sollte nach DSGVO klappen ;-)


8:00
My Application
DASU APP
NEUER DATENKONTAKT
ÜBERSICHT
ABMAHNGENERATOR
letzter Datenkontakt : 19/10/2018
www.dirkihnen.de
mit FakeID 2 angemeldt
NEUE FAKEID ANLEGEN


ORGANIZE!
digitalcourage.de
PoliShirts.de

Digitales Karate

4. DAN stetig entwickeln und anwenden

Danke für Ihre Aufmerksamkeit

Danke an Stefan Macke

Fragen kann ich aus Gründen des Datenschutzes nicht beantworten