Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

# Technischer Datenschutz

Dr. Ronald Petrlic

# Vorstellung

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

- Promovierter Informatiker
- Seit 2015 beim LfDI
- Stellvertretender Referatsleiter im Referat Technisch-organisatorischer Datenschutz, Datensicherheit
- Zuständig für nicht-öffentlichen Bereich
- Durchführung von Projekten
- Mitarbeit zum Thema „Vernetztes Fahren“ auf europäischer Ebene

# Gliederung

- Privacy by Design
- Sicherheit der Verarbeitung
- Häufig gestellte Fragen

# Gliederung



- Privacy by Design
- Sicherheit der Verarbeitung
- Häufig gestellte Fragen

# PbD: Die Anfänge

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

- ANN CAVOUKIAN (DS-Beauftragte von Ontario, Kanada) prägt um 1995 Begriff „*Privacy by Design*“ (PbD)

- „**7 Foundational Principles**“
  - Proaktiv und präventiv
  - Datenschutz als Standard-Einstellung
  - Einbettung des Datenschutzes in das Design
  - Volle Funktionalität
  - Durchgängige Sicherheit: Schutz während des gesamten Lebenszyklus
  - Sichtbarkeit und Transparenz
  - Respekt für Datenschutz

- Problem: Prinzipien charakterisieren Datenschutz-**Eigenschaften**; keine Maßnahmen zur Umsetzung

# PbD in der DS-GVO

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

- PbD in DS-GVO fest verankert
  - **Artikel 25, Abs. 1: Datenschutz durch Technikgestaltung**
  - „Unter Berücksichtigung des **Stands der Technik**, der **Implementierungskosten** und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen **Risiken** für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung **geeignete technische und organisatorische Maßnahmen** – wie z. B. Pseudonymisierung –, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa **Datenminimierung wirksam umzusetzen** und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.“

# PbD: ENISA-Report

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

- *Europäische Agentur für Netz- und Informationssicherheit (ENISA)* gibt 2015 Empfehlungen zur Umsetzung
  - Ziel: Lücke zwischen rechtlichen Vorgaben und vorhandener Technologie schließen

- Allgemeine Empfehlungen (Auszug)
  - Politik soll Anreize für datenschutzfördernde Technologien schaffen
  - Interdisziplinäre Forschung an datenschutzfördernden Technologien
  - Entwickler sollen Werkzeuge zur einfachen Implementierung von Datenschutzmaßnahmen entwickeln
  - DS-Aufsichtsbehörden sollen Beratung und Bewertung von Werkzeugen zur datenschutzgerechten Systemgestaltung vornehmen

- Datenschutzfördernde Technologien
  - *Attribute-based Credentials, Private Information Retrieval, Searchable Encryption, Homomorphic Encryption, Oblivious Transfer, Differential Privacy, Onion Routing, Virtual Private Networks, Transport Layer Security, etc.*

# PbD: Offene Fragen

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

- Offene Fragen (u. A.)
  - Was ist der in der DS-GVO erwähnte **Stand der Technik**?
    - Vorschlag vom EU-Parlament: „neueste technische Errungenschaften“ wurde nicht berücksichtigt
    - Sind *Attribute-based Credentials, Private Information Retrieval, Searchable Encryption, Homomorphic Encryption, Oblivious Transfer, Differential Privacy, etc.* schon Stand der Technik?
    - Oder bleiben nur TLS, VPNs,… übrig?
  - Inwieweit können DS-Aufsichtsbehörden der ENISA-Empfehlung zu Beratung und Bewertung nachkommen?
    - Problem: Ausstattung der Aufsichtsbehörden im Bereich Technik
      - BW: 1 „Techniker“ kommt auf ~450.000 Unternehmen
      - Österreich: 0 Techniker in der DS-Aufsichtsbehörde

# PbD im Web?

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

- MARIT HANSEN (Leiterin ULD Schleswig-Holstein) in einem Interview in der *PinG 01/2016*:
  - „Ob man gleich das maximale *Privacy by Design* erreichen kann – in jeder Hinsicht einen Riesenschritt zu gehen, wenn viele bei den kleinen Schritten noch gar nicht mitkommen –, da habe ich so meine Zweifel. […] Mich erschreckt es, dass selbst unter den datenschutzbewussten Institutionen – […] **noch nicht einmal eine simple SSL/TLS-Verschlüsselung des Webauftritts vorhanden** ist. Dies wäre für mich noch lange nicht wirkliches Privacy by Design, aber doch ein **Minimum an technisch-organisatorischen Maßnahmen nach dem Stand der Technik**.“

→ kommen später noch darauf zu sprechen!

# PbD im Internet der Dinge?

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

- **GPEN Privacy Sweep 2016**
  - 25 DS-Aufsichtsbehörden prüfen 300 IoT-Geräte
  - LfD BW prüft Geräte von Herstellern aus BW
  - ~60 % der Nutzer werden nicht hinreichend aufgeklärt, welche personenbezogenen Daten erhoben werden und was mit ihnen geschieht
    - Meist keine DS-Erklärung für Geräte verfügbar

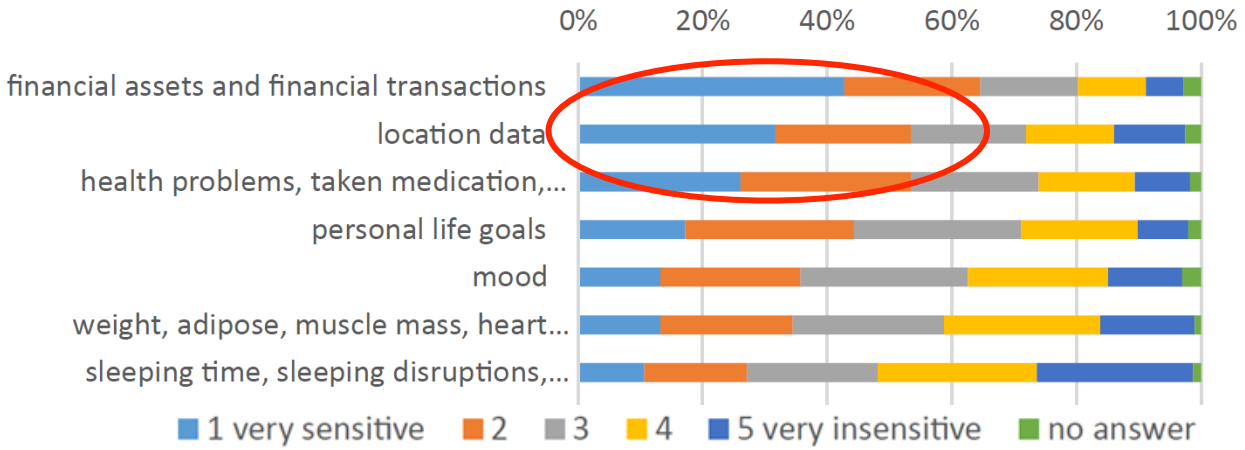
**Pressemitteilung LfD BW**: „Datenschutz beim Internet der Dinge – Klein und nicht fein!“ (September 2016)

# PbD beim Quantified Self?

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

- Wie denken Nutzer über Datenschutz?
  - Umfrage unter 400 Briten im Februar 2016
    - 75% besorgt über Transfer von **Gesundheitsdaten** an Diensteanbieter
    - 76% besorgt über Transfer von **Aufenthaltsort** an Diensteanbieter
    - 88% besorgt über Transfer von **Finanzdaten** an Diensteanbieter

    - Sensibilität der Daten:




**Veröffentlichungen**:
- LEIBENGER, MÖLLERS, PETRLIC A., PETRLIC R., SORGE:
"Privacy Challenges in the Quantified Self Movement – An EU Perspective", *Proc. on Privacy Enhancing Technologies*, 2016
- PETRLIC: „Das vermessene Selbst", *Datenschutz und Datensicherheit (DuD)*, Heft 2/2016, Springer.

# PbD beim Quantified Self?

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

| | QS Tool | Data Exclusively Stored in Cloud | Login | | | Additional Mandatory Data | | | | Data Uses | | | | | | Data Transfer | | | | | | | | Place of Business | Policy Features | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Email | Telephone Number | 3rd Party Provider | Email Address | Real Address[1] | Real Name[1] | Other Personal Data[2] | Notifications | Improvement of Service[3] | Personalized Advertisement | Direct Advertisement | ... Explicitly Stated | Research | Public by Default[4] | To Service Providers | Service Providers Bound by Policy | To Involved 3rd Parties[5] | To Uninvolved 3rd Parties[6] | ... Only Anonymized/Aggregated | Google Analytics/Social Media Buttons | Google Analytics IP Anonymization | | Email Notification on Changes | Data Usage Rights Revokable | Provider May Modify Information | User May Access/Rectify Information |
| Sport/ Gesundheit | Runtastic | | ✓ | | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | | ✓ | | | | ✓ | ✓ | ✓ | ✓ | Austria | | | ✓ | |
| | Withings | ✓ | ✓ | | | ✓ | | ✓ | ✓ | ✓ | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | | | ✓ | ✓ | France | | ✓ | | ✓ |
| Aufenthaltsort | Foursquare | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | | USA (NY) | ✓ | ✓ | | ✓ |
| | Goodreads | ✓ | ✓ | | ✓ | ✓ | | ✓ | | ✓ | | | ✓ | | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | | USA (CA) | | | | ✓[7] |
| Finanz | Mint | ✓ | ✓ | | | ✓ | ✓ | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ | | | USA (CA) | | ✓ | | ✓[7] |
| | RescueTime | ✓ | ✓ | | ✓ | ✓ | | | | ✓ | | | | | | | | | | | | ✓ | | USA (WA) | ✓ | ✓ | | |
| Gesundheit | CureTogether | ✓ | ✓ | | | ✓ | | | | ✓ | ✓ | | ✓ | | ✓ | | | | | ✓ | ✓ | ✓ | | USA (CA) | ✓ | ✓ | | |
| | MoodPanda | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | | UK | | ✓ | | ✓ |

# PbD: Aktueller Stand

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

- Es besteht große Kluft zwischen Forschung und Praxis
  - Wurde bei „*Smart Metering*“ besonders deutlich
    - Kritik aus Datenschutzsicht seit 2010
    - Zahlreiche Forschungsprojekte / Google Scholar offenbart tausende wissenschaftliche Arbeiten zum Thema
    - Im Gesetz zur Digitalisierung der Energiewende von 2015 ist insgesamt 4 mal von „Privacy by Design“ die Rede
      - „privacy-by-design-Standard“ des BSI soll dies gewährleisten

      → PbD allerdings nicht erkennbar

      (lediglich Verschlüsselung / Standard-„TOMs“)

# Unsere Arbeiten zu PbD

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

- Datenschutzfreundliches **Offline-Tracking**
  - Neues Phänomen: Nutzer werden in Kaufhäusern und Städten „getrackt“ (über WiFi und Bluetooth-Signale)
    - Je nach Ausgestaltung: weder Einwilligung noch Widerspruch möglich und damit unzulässig
  - Projekt „*Smart Urban Services*“: Stadtlabor Reutlingen
    - Unser Ziel: Durch technischen Datenschutz Anonymität der Bürger gewährleisten
    - Unser Beitrag: Mehrstufiges Anonymisierungsverfahren (sowohl in den Sensorknoten als auch vor Veröffentlichung der Daten)

# PbD in der Praxis

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

- **Social Plugins** (*Facebook Like*, *Twitter Timeline*, etc.)
  - Einbindung der Standard-Plugins problematisch

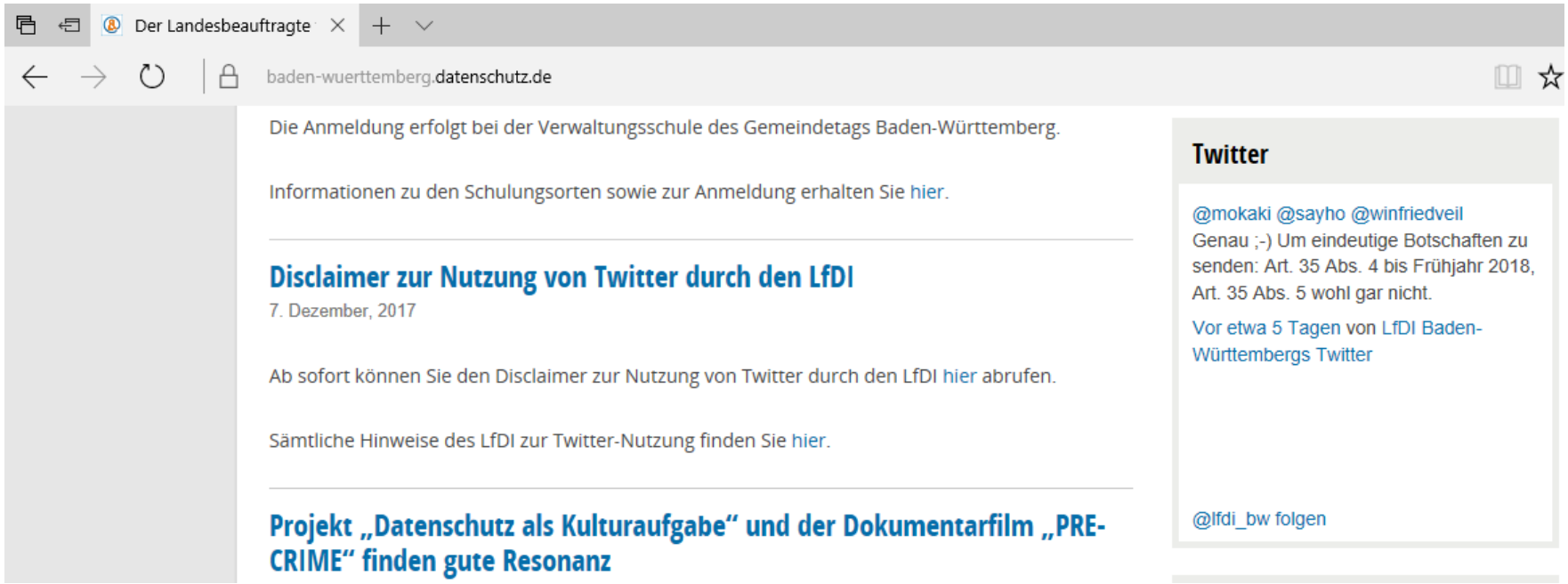

    → bei Aufruf der Webseite werden Daten an soziales Netzwerk übermittelt

  - Aktueller Stand (Anfang 2018) in BW
    - ~40.000 Unternehmens-Websites geprüft
      - Bei 5 % der Seiten: aktives Facebook-Plugin
      - Bei 1 % der Seiten: aktives Twitter-Plugin
    - ~1.700 Behörden-Websites geprüft
      - 8 aktive Twitter-Plugins
      - 18 aktive Facebook-Plugins

# PbD in der Praxis

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

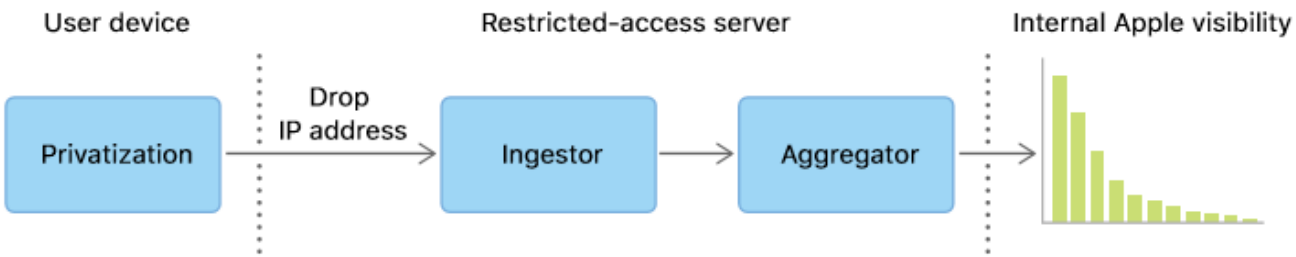
- Datenschutzfreundliche Alternative
  - *2-Klick-Lösung / Shariff-Lösung*
    - Skript auf Webserver als Vermittler zwischen sozialem Netzwerk und Nutzer → erst bei Klick auf Plugin gehen Daten an soziales Netzwerk



# PbD in der Praxis

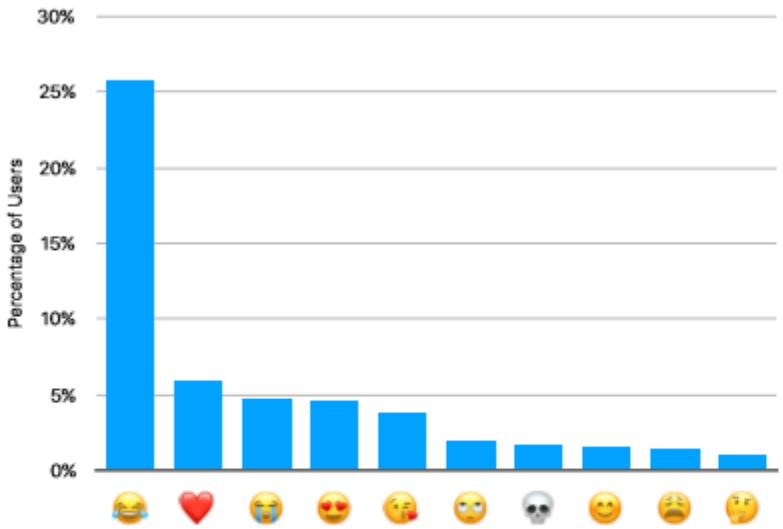
Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

- **Nutzungsanalyse bei Apple iOS/macOS**
  - Wohl größter Einsatz von PbD in der Praxis (hunderte Millionen Geräte)
    - Nutzungsdaten mittels *Differential Privacy* „verrauscht“ an Apple übermittelt
    - U.A.: Ermittlung der populärsten Emoji, Erkennen von häufig genutzten Wörtern (die bisher nicht im Wörterbuch sind), Vorhersage über gewolltes Auto-Play von Videos auf Websites, etc.

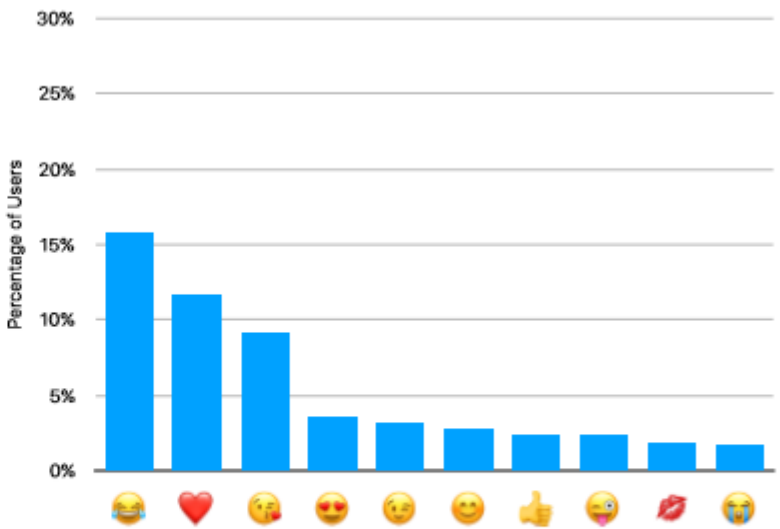


# PbD in der Praxis

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg




(a) English




(b) French

Figure 5: Emojis in Different Keyboard Locales

# PbD in der Praxis

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

- **Elektronischer Personalausweis**
  - *Restricted Identification*
    - Ausweis-Inhaber tritt gegenüber Diensteanbietern mit unterschiedlichen Identifikatoren (unter Pseudonym) auf → kein Tracking über mehrere Dienste hinweg möglich!
  - Altersverifikation, ohne genaues Geburtsdatum bekannt zu geben
  - Lehrstück für PbD!
    - In der Praxis allerdings kaum genutzt…

# PbD: Offene Forschungsfragen

- **Instant Messaging** (bspw. *WhatsApp*)
  - Ende-zu-Ende-Verschlüsselung inzwischen „Standard“

    (im Gegensatz zu E-Mail-Kommunikation)

  - Aber: um festzustellen, welche eigenen Kontakte einen Messenger ebenfalls nutzen, muss das Telefonbuch an den Dienst zum Abgleich der Tel.nr. übermittelt werden
    - Hierfür gibt es noch keine praktikable, datenschutzfreundliche Lösung

# Privacy by Default

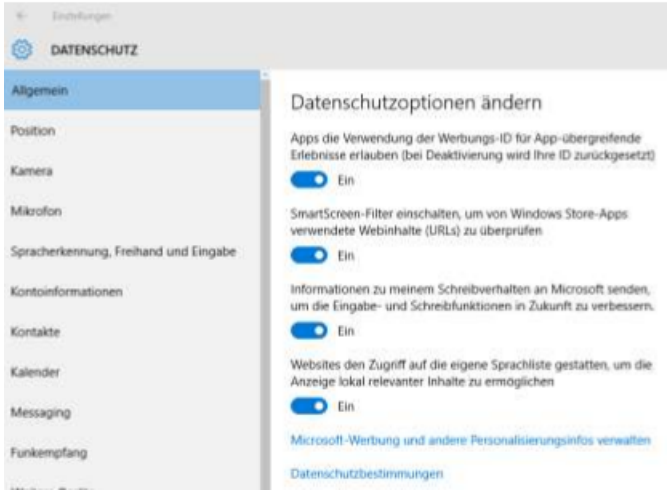
Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

- Teilaspekt der *Foundational Principles* von Privacy by Design
  - „Datenschutz als Standard-Einstellung“

- Idee: Nutzer müssen Datenschutz-Einstellungen nicht selbst vornehmen (datenschutzfreundliche Voreinstellung)

- **Gegenbeispiel**: *Windows 10*
  - Nutzer müssen Datenübermittlung an Microsoft

nach Installation des Systems selbst deaktivieren



# Gliederung



- Privacy by Design
- Sicherheit der Verarbeitung
- Häufig gestellte Fragen

# Sicherheit der Verarbeitung

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

- Artikel 32 DS-GVO: Sicherheit der Verarbeitung
  - Weitestgehend bekannt (§ 9 samt Anlage BDSG-alt)
  - Neu: Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Abs. 1 d))

    → Penetration Tests!
  - Außerdem: Nichteinhaltung der Vorgaben nun bußgeldbewährt!
  - Empfehlung: Orientierung an Empfehlungen und Technischen Richtlinien des BSI (Verpflichtung nur für öffentliche Stellen i.R.v. § 64 BDSG)

→ Maßnahmen sollen ein **dem Risiko angemessenes Schutzniveau** gewährleisten

# Projekt: SSL/TLS-Check

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

- Projekt 2016 gestartet: seitdem regelmäßiger Test von ~40.000 Unternehmens-Websites in BW
  - Ziel: Großflächige Prüfung der Einhaltung der rechtlichen Vorgaben in Bezug auf „Verschlüsselung der Website“
    → Verbesserung der Sicherheit für Nutzer
  - Bei Abfrage personenbezogener Daten (bspw. Kontaktformular, Onlineshop, etc. Pflicht zur Verschlüsselung!)
  - TLS (Transport Layer Security) als **das** Sicherheitsprotokoll im Internet
    - Bietet Vertraulichkeit, Authentizität und Integrität bei der Kommunikation

| sehr unsicher | unsicher |
|---|---|
| SSL V2.0 | SSL V3.0 |

**Nicht mehr sicher nach dem Stand der Technik**

| mittel | sicher | sehr sicher |
|---|---|---|
| TLS 1.0 | TLS 1.1 | TLS 1.2 |

**BSI-Vorgabe!**

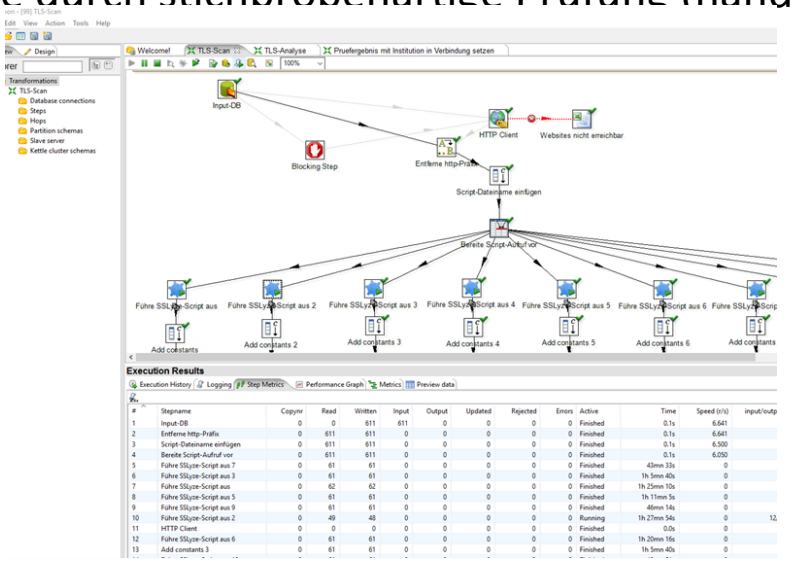
Als Übergangslösung noch in Ordnung

Quelle: Pohlmann, https://www.stuttgart.ihk24.de/blob/sihk24/Fuer-Unternehmen/innovation/downloads/3300070/801b0ef29405c1710223f9a76bc24c06/TLS-Check-Ergebnisse-data.pdf

# Projekt: SSL/TLS-Check

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

- Eigene Entwicklung einer Prüfplattform, basierend auf Business Intelligence-Werkzeug
  - Komplexe Prüftätigkeiten „einfach“ durchführbar (auch durch Nicht-Techniker)
  - Modularer Ansatz → können rasch weitere Prüfkriterien mit einbeziehen
  - Verwendung gängiger Werkzeuge (SSLyze, Nmap, etc.)
  - Qualitätskontrolle durch stichprobenartige Prüfung (händisch und mittels weiterer Tools)



# Projekt: SSL/TLS-Check

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

- Entwicklung im Lauf der Zeit
  - 2016: 5-6 % der Websites über „einigermaßen sichere“ (TLS ab 1.0) HTTPS-Verbindung angeboten
  - 2017: 15 % über HTTPS (ab TLS 1.0)
  - 2018 (Anfang): 22 % über HTTPS (ab TLS 1.0)

- Verbesserung deutlich erkennbar
  - Zahl der Beschwerden hat ebenfalls stark zugenommen → Verantwortliche i.d.R. kooperativ
  - Anteil an „Let‘s Encrypt“-Zertifikaten inzwischen bei 30 % (2017: 26 %, 2016: 7 %)
  - Aber: lediglich 10 Websites halten BSI-Vorgaben ein! (2017: 3, 2016: 0)

**Veröffentlichung**:
- PETRLIC, MANNY: „Wie sicher ist der Zugriff auf Websites im Internet?“, *Datenschutz und Datensicherheit (DuD)*, Heft 02/2017, Springer.

# Projekt: SSL/TLS-Check

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

- Situation bei Behörden-Websites
  - Prüfung von 1.754 Websites
  - 2017: 13 % über HTTPS, 2018: 19 % über HTTPS

| Behörde | Anzahl Websites | HTTPS (2017) | HTTPS (2018) |
|---|---|---|---|
| Hochbauamt | 25 | 4 % | 8 % |
| Notariat | 317 | 0 % | 0 % |
| Landratsamt | 35 | 31 % | 43 % |
| Ministerium | 11 | 64 % | 64 % |
| Stadt/Gemeinde | 1.054 | 11 % | 28 % |
| Amtsgericht | 108 | 0 % | 0 % |
| Arbeitsgericht | 17 | 0 % | 0 % |
| Finanzamt | 82 | 0 % | 0 % |

**Veröffentlichung**:
- PETRLIC: „HTTPS im Lichte der DSGVO“, *Datenschutz und Datensicherheit (DuD)*, Heft 11/2018, Springer.

# Projekt: SSL/TLS-Check

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

- Situation bei Behörden-Websites
  - Von 311 Websites von Städten sind 43 % per HTTPS gesichert
  - Von 743 Websites von Gemeinden sind 20 % per HTTPS gesichert

| Einwohnerzahl | Anzahl Web-sites | HTTPS (2018) | Bevölkerung |
|---|---|---|---|
| < 2.000 | 187 | 9 % | 222.073 |
| 2.000 – 5.000 | 403 | 21 % | 1.356.508 |
| 5.000 – 20.000 | 412 | 34 % | 3.819.913 |
| 20.000 – 50.000 | 78 | 53 % | 2.406.106 |
| 50.000 – 100.000 | 13 | 62 % | 902.132 |
| 100.000 – 500.000 | 8 | 100 % | 1.459.920 |
| > 500.000 | 1 | 100 % | 615.862 |

# Gliederung



- Privacy by Design
- Sicherheit der Verarbeitung
- Häufig gestellte Fragen

# Häufig gestellte Fragen

- Darf Windows 10 im Unternehmen eingesetzt werden?
  - Ja!
    - Aus Sicherheitssicht sinnvoll, aktuelle Systeme zu nutzen
    - Empfehlung: Enterprise-Version / Deaktivieren der Datenübermittlungen mittels Gruppenrichtlinien
    - „Orientierungshilfe zur datenarmen Konfiguration von Windows 10“ der AKIF-Gruppe der deutschen Forschungseinrichtungen

# Häufig gestellte Fragen

- Dürfen E-Mails mit personenbezogenen Daten noch ohne Ende-zu-Ende-Verschlüsselung an Nutzer versendet werden?
  - Ja!
    - Aber: Risiko prüfen!
      - Bei sensiblen Daten: Alternativen bieten (bspw. Online-Portal, PDF-Verschlüsselung, …)
    - Sicherstellen, dass Mailserver Transportverschlüsselung nach Stand der Technik unterstützt!
      - Empfehlung: *BSI TR-03108* („Sicherer E-Mail-Transport“)

→ **Könnte in unsere großflächige Prüfung aufgenommen werden**

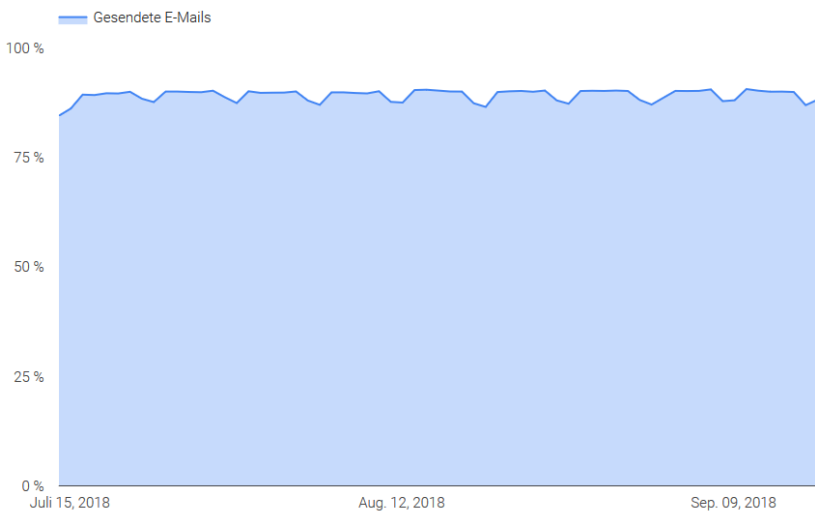
# Häufig gestellte Fragen

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

- *Google Transparency Report*: E-Mail-Verschlüsselung bei Übertragung

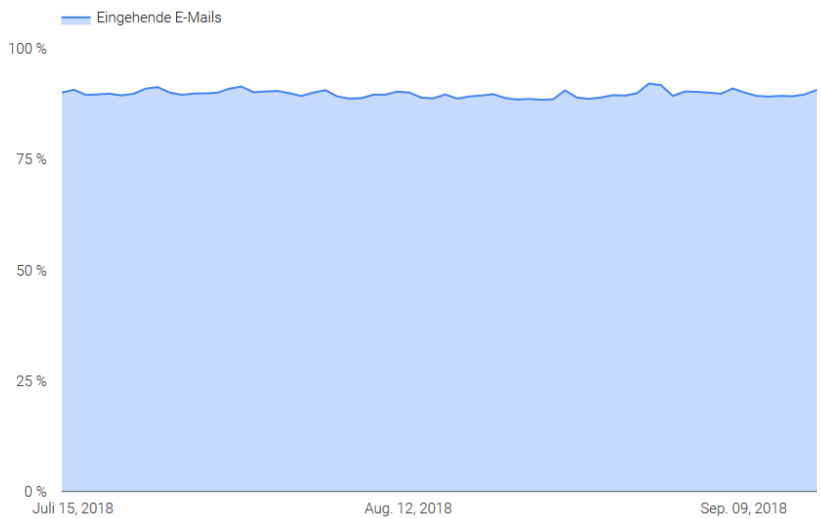
Verschlüsselte ausgehende E-Mails: 88 %

ANFANG 14.7.2018 ENDE 12.10.2018




Verschlüsselte eingehende E-Mails: 93 %

ANFANG 14.7.2018 ENDE 12.10.2018




- „E-Mail Made in Germany“: Mail-Transport TLS-geschützt

# Häufig gestellte Fragen

- Müssen personenbezogene Daten auf dem Rechner verschlüsselt werden?
  - Ja!
    - Einfach umzusetzen (über Betriebssystem)
    - Rechner gehen verloren oder werden gestohlen (zahlreiche Datenpannenmeldungen)
    - Vorteil: Benachrichtigung an Betroffene (Art. 34) muss nicht erfolgen

# Häufig gestellte Fragen

- Dürfen Passwörter auf Server-Seite im Klartext gespeichert werden?
  - Nein!
    - Speicherung von Nutzer-Passwörtern ausschließlich als „Salted Hash“-Werte (seit Jahren Stand der Technik!)
    - Mit Hacking-Angriffen auf Server-Datenbanken muss gerechnet werden

# Häufig gestellte Fragen

- Wie kann ein Nutzer identifiziert werden, der von seinen Betroffenenrechten (Art. 15ff) Gebrauch machen möchte?
  - Ausgangslage: Elektronischer Weg ausdrücklich erlaubt (Art. 12)
  - Problem: eindeutige Identifizierung des Betroffenen (E-Mail-Adresse i.d.R. nicht ausreichend)
  - Geschwärzte Ausweiskopie kann verlangt werden (elektronische Bereitstellung: auf Sicherheit der Übertragung achten)
  - Einfacher Fall: Online-Konto – auf zusätzliche Identifizierung kann verzichtet werden; allerdings: aus Sicherheitssicht 2-Faktor-Authentifizierung sinnvoll

# Häufig gestellte Fragen

- Wie kann eine Datenschutz-Folgeabschätzung durchgeführt werden?
  - Angelehnt an ISO 29134
  - Praktikabel: Guidelines und Tool der CNIL (BayLfD arbeitet an deutscher Version des Tools)
  - Außerdem hilfreich: Musterbeispiel „Insight AG“ vom LDA Bayern
  - Wenig hilfreich: SDM

# Zusammenfassung und Ausblick

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

- Es gibt noch einiges zu tun im Bereich des technischen Datenschutzes
  - Es braucht mehr Techniker als DSB und in den Aufsichtsbehörden
  - Mehr Austausch mit der Wissenschaft → Entwicklung **praktikabler** Lösungen
  - Es wird dauern, bis sich PbD in der Praxis durchsetzt / auf Hersteller niederschlägt
  - Stand der Technik zu bestimmen wird nicht einfacher werden…

# Vielen Dank für Ihre Aufmerksamkeit

petrlic@lfdi.bwl.de