TECHNISCHE UNIVERSITÄT DARMSTADT

# DATENSCHUTZ IN AMI-SYSTEMEN

Ambient Intelligence - Vorlesung 11

TECHNISCHE UNIVERSITÄT DARMSTADT

# AGENDA

1 Begriffsbestimmungen

2 Problembeschreibung

3 Datenschutzgrundlagen

4 Datenschutz und Ambient Intelligence

5 Lernziele

TECHNISCHE UNIVERSITÄT DARMSTADT

KAPITEL 1

# BEGRIFFSBESTIMMUNGEN

TECHNISCHE UNIVERSITÄT DARMSTADT

# DATENSCHUTZ

„Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten“

[EU-Datenschutz-Grundverordnung 2016/679 (DSGVO, *General Data Protection Regulation (GDPR)*)
https://eur-lex.europa.eu/eli/reg/2016/679/oj]

TECHNISCHE UNIVERSITÄT DARMSTADT

# PERSONENBEZOGENE DATEN

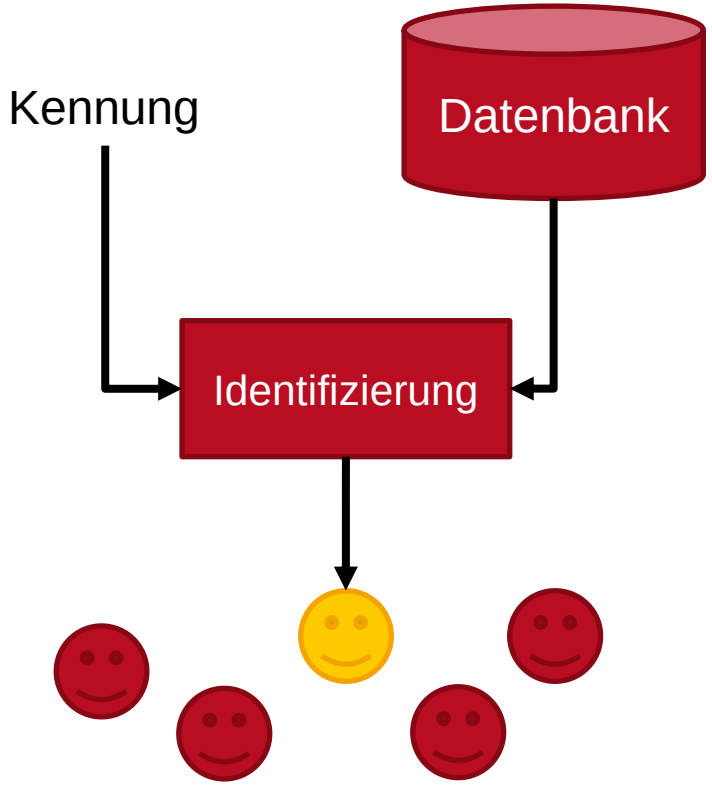
alle Informationen, die sich auf identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen

TECHNISCHE UNIVERSITÄT DARMSTADT

# IDENTIFIZIERBARKEIT

direkt oder indirekt, insbesondere unter Bezugnahme auf eine Kennung wie

- einen Namen
- eine Kennnummer
- Standortdaten
- eine Online-Kennung
- ein oder mehrere besondere Merkmale, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität einer natürlichen Person sind



TECHNISCHE UNIVERSITÄT DARMSTADT

KAPITEL 2

# PROBLEMBESCHREIBUNG

TECHNISCHE UNIVERSITÄT DARMSTADT

# ERFASSUNG PERSONENBEZOGENER DATEN

Personenbezogene Daten sind erforderlich für die Erfüllung vieler Aufgaben

| Aufgabe | Benötige personenbezogene Daten |
|---|---|
| Teilnahme am Mobilfunknetz | Internationale Mobile Subscriber Identity (IMSI) |
| Zugriff auf Webseiten | Client-IP-Adresse |
| eCommerce | z.B. Lieferadresse, Kreditkartennummer,… |
| eGovernment | z.B. Steueridentifikationsnummer,… |
| Personalisierung von Werbung | Client-IP-Adresse und Informationen über Nutzer |
| … | … |

TECHNISCHE UNIVERSITÄT DARMSTADT

# BEDROHUNGEN

- Missbrauch oder Preisgabe personenbezogener Daten
- Unterwerfung unter Entscheidungen, die ausschließlich auf automatisierter Datenverarbeitung – einschließlich Profiling – beruhen
- Identitätsbetrug
- Überwachung durch staatliche Stellen

TECHNISCHE UNIVERSITÄT DARMSTADT

# PROFILING

automatisierte Verarbeitung personenbezogener Daten, um bestimmte persönliche Aspekte zu bewerten oder vorherzusagen, insbesondere bezüglich

- Arbeitsleistung
- wirtschaftliche Lage
- Gesundheit
- persönliche Vorlieben
- Interessen
- Zuverlässigkeit
- Verhalten
- Aufenthaltsort oder Ortswechsel einer natürlichen Person

TECHNISCHE UNIVERSITÄT DARMSTADT

KAPITEL 3

# DATENSCHUTZGRUNDLAGEN

TECHNISCHE UNIVERSITÄT DARMSTADT

# DATENSCHUTZRECHT – KURZE GESCHICHTE

**Vor EDV:**

- Verschwiegenheitspflicht für Heilberufe, Anwälte, Amtsträger,…

*„Was ich bei der Behandlung sehe oder höre oder auch außerhalb der Behandlung im Leben des Menschen, werde ich, soweit man es nicht ausplaudern darf, verschweigen und solches als ein Geheimnis betrachten.“ (Eid des Hippokrates)*

**EDV-Zeitalter:**

- Immer mehr Daten, die nahezu unbegrenzt gespeichert, verknüpft und ausgewertet werden können
- **1977:** Erste Fassung des Bundesdatenschutzgesetzes
- **1983:** Volkszählungsurteil: „Recht auf informationelle Selbstbestimmung“ als Ausprägung des allgemeinen Persönlichkeitsrechts als Grundrecht
- **1995:** EU-Datenschutzgrundlinie → Umsetzung in nationales Recht durch Änderung des Bundesdatenschutzgesetzes
- **2016:** EU-Datenschutz-Grundverordnung (mit allgemeiner Gültigkeit und unmittelbarer Wirksamkeit in der EU)

TECHNISCHE UNIVERSITÄT DARMSTADT

# RECHT AUF INFORMATIONELLE SELBSTBESTIMMUNG

Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen

**Begründung:**

Die freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. [Volkszählungsurteil 1983]

TECHNISCHE UNIVERSITÄT DARMSTADT

# CHARTA DER GRUNDRECHTE DER EU (2012/C 326/02) [https://eur-lex.europa.eu/eli/treaty/char_2012/oj]

**Artikel 8 – Schutz personenbezogener Daten**

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und

mit Einwilligung der betroffenen Person oder

auf einer sonstigen gesetzlich geregelten legitimen Grundlage

verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

(Datenschutzbeauftragte)

# NICHTS ZU VERBERGEN?

TECHNISCHE UNIVERSITÄT DARMSTADT

*„Arguing that you don‘t care about the right to privacy because you have nothing to hide is no different than saying you don‘t care about free speech because you have nothing to say.“*

Edward Snowden,
ehemaliger CIA-Mitarbeiter, enthüllte 2013, dass die US-Geheimdienste verdachtsunabhängig weltweit private Daten sammeln.
[https://www.eff.org/nsa-spying/nsadocs]

TECHNISCHE UNIVERSITÄT DARMSTADT

# VERARBEITUNG PERSONENBEZOGENER DATEN

Nach **DSGVO Artikel 6** nur erlaubt, wenn mindestens eine der folgenden Bedingungen erfüllt ist:

- betroffene Person hat ihre Einwilligung gegeben

- zur Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen erforderlich
- zur Erfüllung einer rechtlichen Verpflichtung erforderlich
- zum Schutz lebenswichtiger Interessen erforderlich
- zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe erforderlich
- zur Wahrung von berechtigen Interessen des für die Datenverarbeitung Verantwortlichen erforderlich, sofern nicht die Interessen oder Grundrechte der betroffenen Person Vorrang haben

} sonstige gesetzlich geregelte legitime Grundlage

# EINWILLIGUNG DER BETROFFENEN PERSON

Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung,

- mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, und
- die sie freiwillig für einen bestimmten Zweck, in informierter Weise und unmissverständlich abgibt

Kann jederzeit widerrufen werden!

# EINWILLIGUNG IN DER PRAXIS

- Häufig Klickfenster zur Einwilligung in die Nutzung von Tracking-Cookies zur Sammlung von Daten über Interessen, Vorlieben und Gewohnheiten
- Benutzer können ihre Einwilligung in die Verarbeitung personenbezogener Daten gegen kostenlose Dienstleistungen eintauschen

TECHNISCHE UNIVERSITÄT DARMSTADT

# „BERECHTIGTE“ INTERESSEN

Können Vorrang haben vor den Interessen oder Grundrechten der betroffenen Person

**Beispiele:**

- Verarbeitung personenbezogener Daten von Kunden in dem Umfang, der für die Verhinderung von Betrug erforderlich ist
- Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung

TECHNISCHE UNIVERSITÄT DARMSTADT

# BESONDERS GESCHÜTZTE PERSONENBEZOGENE DATEN

- Personenbezogene Daten, aus denen
  - die ethnische Herkunft
  - politische Meinungen
  - religiöse oder weltanschauliche Überzeugungen
  - die Gewerkschaftszugehörigkeit

  hervorgehen
- genetische Daten
- biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person

TECHNISCHE UNIVERSITÄT DARMSTADT

# BESONDERS GESCHÜTZTE PERSONENBEZOGENE DATEN

nach **DSGVO Artikel 9** ist Verarbeitung untersagt, es sei denn

- betroffene Person hat für bestimmte Zwecke ausdrücklich eingewilligt
- erforderlich, um Rechte auszuüben und Pflichten nachkommen zu können
- zum Schutz lebenswichtiger Interessen erforderlich und betroffene Person ist außerstande, ihre Einwilligung zu geben
- sie erfolgt durch eine Organisation ohne Gewinnerzielungsabsicht ausschließlich auf Mitglieder der Organisation bezogen und die Daten gelangen nicht nach außen
- betroffene Person hat die Daten öffentlich gemacht
- bei Handlungen der Gerichte im Rahmen ihrer Tätigkeit erforderlich
- auf gesetzlicher Grundlage aus Gründen erheblichen öffentlichen Interesses erforderlich
- für Zwecke im Gesundheits- oder Sozialbereich auf gesetzlicher Grundlage oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs erforderlich
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit auf gesetzlicher Grundlage erforderlich
- auf gesetzlicher Grundlage für im öffentlichen Interesse liegende Archivzwecke, für Forschungszwecke oder für statistische Zwecke erforderlich

TECHNISCHE UNIVERSITÄT DARMSTADT

# ALLGEMEINE DATENSCHUTZGRUNDSÄTZE

- Zweckbindung
- Datenminimierung
- begrenzte Speicherfristen
- Datenqualität
  - für den beabsichtigten Zweck relevant
  - korrekt
  - vollständig
  - auf dem neuesten Stand
- Datenschutz durch Technikgestaltung (*Data Protection / Privacy by Design*)
- datenschutzfreundliche Voreinstellungen

# DATENSCHUTZ DURCH TECHNIKGESTALTUNG

TECHNISCHE UNIVERSITÄT DARMSTADT

geeignete technische und organisatorische Maßnahmen, um Datenschutzgrundsätze wirksam umzusetzen, z.B.

- Pseudonymisierung
- Sicherheit von Vertraulichkeit und Integrität

unter Berücksichtigung von

- Stand der Technik
- Implementierungskosten
- Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen

TECHNISCHE UNIVERSITÄT DARMSTADT

# DATENSCHUTZ-FOLGEABSCHÄTZUNG

- Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten
- Vor der Implementierung der vorgesehenen Verarbeitungsvorgänge
- Durchzuführen, wenn die Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat

TECHNISCHE UNIVERSITÄT DARMSTADT

# INHALT EINER DATENSCHUTZ-FOLGEABSCHÄTZUNG

- systematische Beschreibung der geplanten Verarbeitungsvorgänge und Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
- Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen
- zur Bewältigung der Risiken geplante Abhilfemaßnahmen, wobei den Rechten der betroffenen Personen und den berechtigten Interessen Rechnung getragen wird

TECHNISCHE UNIVERSITÄT DARMSTADT

KAPITEL 4

# DATENSCHUTZ UND AMBIENT INTELLIGENCE

TECHNISCHE UNIVERSITÄT DARMSTADT

# DATENSCHUTZ IN AMI-SYSTEMEN

**Ambient Intelligence:** Konvergenz von allgegenwärtigem Computing, allgegenwärtiger Kommunikation und an den Benutzer angepassten Schnittstellen

**Herausforderungen:**

- Benutzer muss bei Inbetriebnahme ausdrücklich in die Verarbeitung personenbezogener Daten einwilligen
- Was ist, wenn mehrere Personen betroffen sind?

TECHNISCHE UNIVERSITÄT DARMSTADT

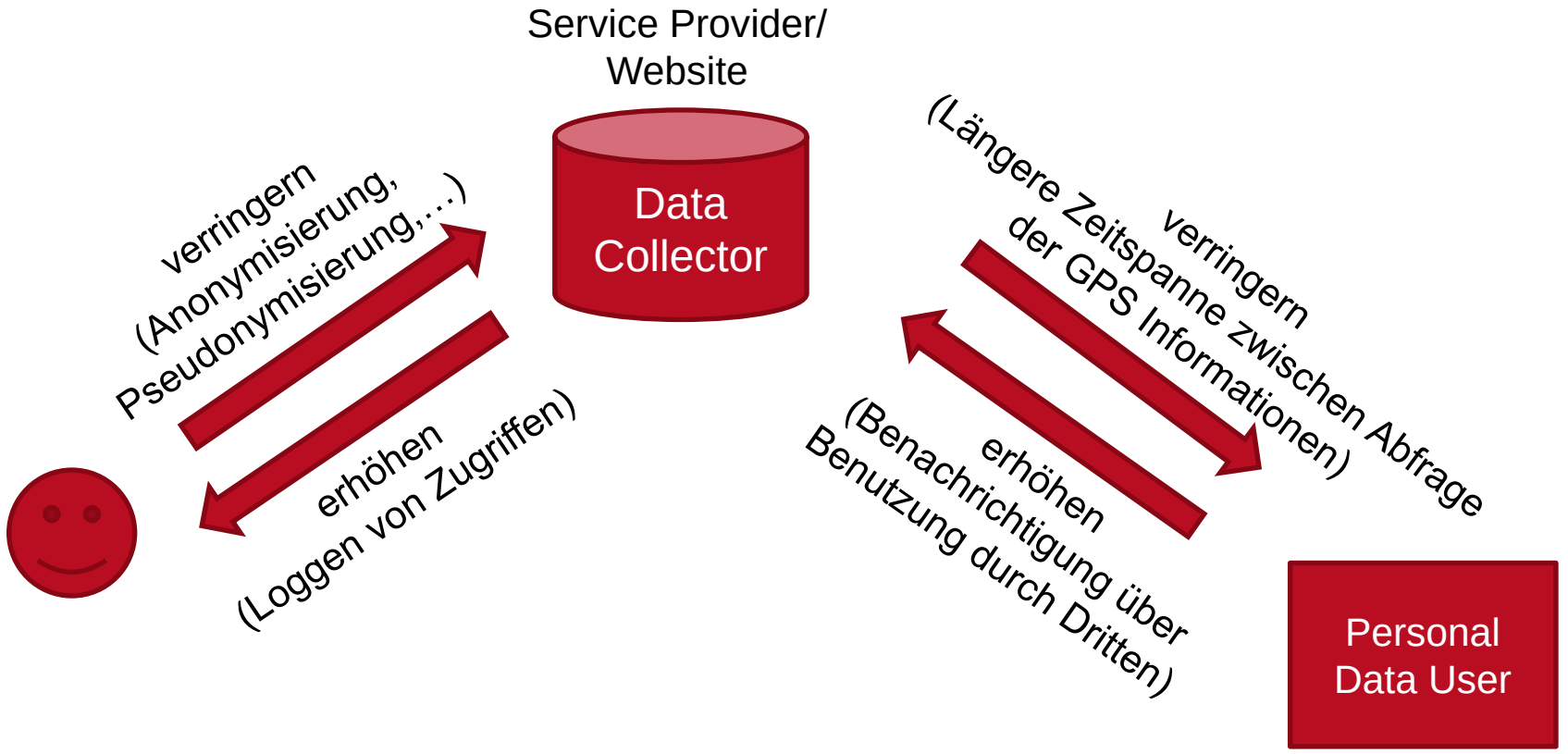
# GRUNDSATZ DER MINIMIERUNG DER ASYMMETRIE

Informationsfluss von der betroffenen Person zum Datensammler verringern

Informationsfluss vom Datensammler zur betroffenen Person steigern

TECHNISCHE UNIVERSITÄT DARMSTADT

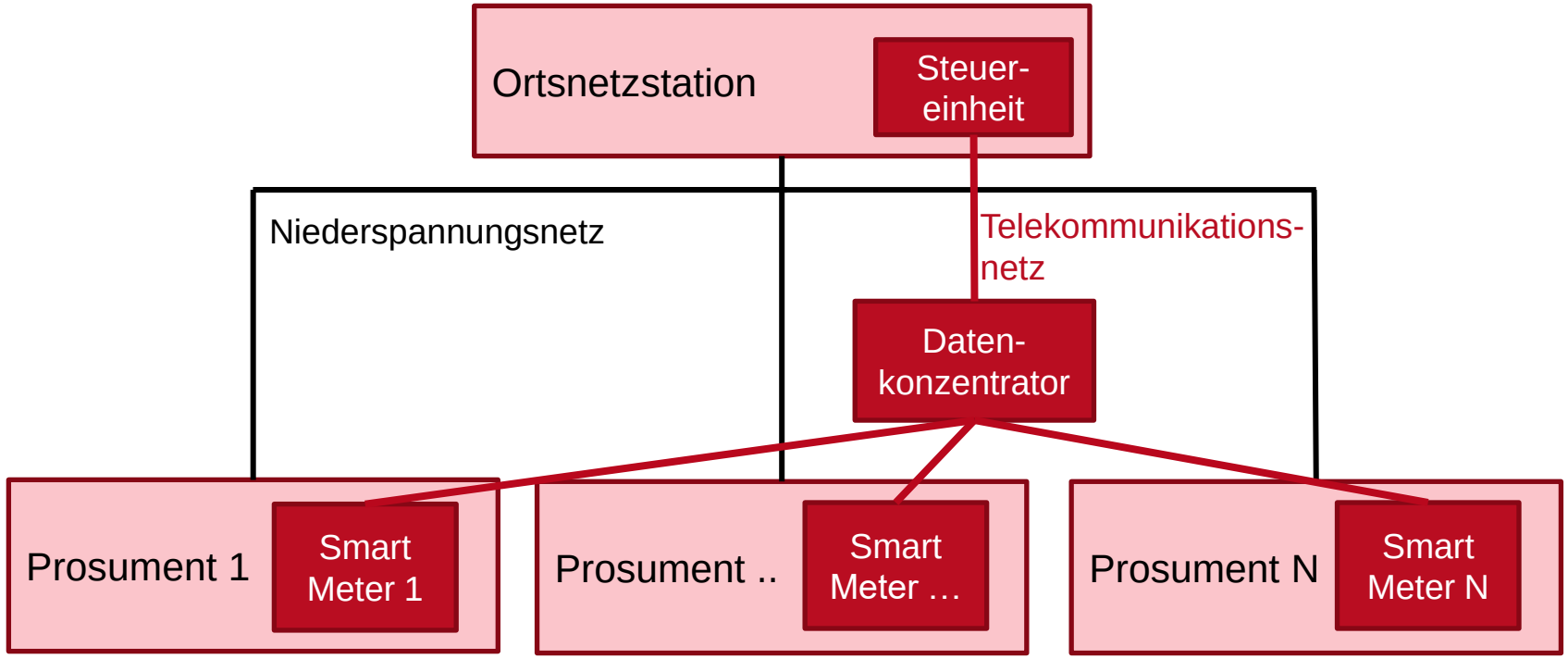
# BEISPIEL: MINIMIERUNG DER ASYMMETRIE



TECHNISCHE UNIVERSITÄT DARMSTADT

# BEISPIEL: AUSSCHNITT AUS DEM SMART GRID

- Smart Meter melden alle 15min Leistungsmesswerte, um Einspeise- und Lastregelung zu ermöglichen
- Der Datenkonzentrator summiert alle zu gleicher Zeit erhobenen Messwerte aus einem Teilnetz um sie zu anonymisieren.



# SICHERHEITSPROBLEM

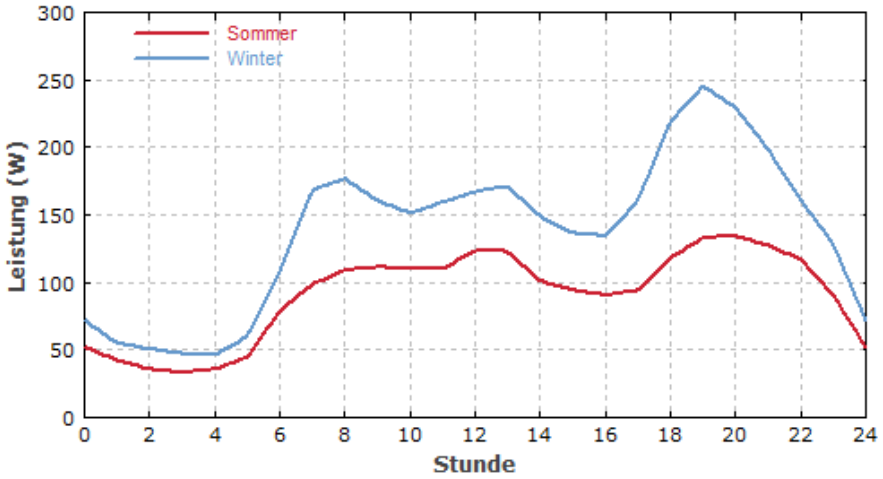
TECHNISCHE UNIVERSITÄT DARMSTADT

**Bedrohung:**

- Smart-Meter-Messwerte erlauben Ausforschung von Abweichungen vom „Normalverbrauch“
- Unbefugte Änderung der Messwerte

**Sicherheitsziel:**

- Vertraulichkeit und Integrität der Smart-Meter-Messwerte sollte im gesamten Verarbeitungsprozess geschützt werden




[http://www.energie-lexikon.info/lastprofil.html]

# SMART-METER-SCHUTZPROFILE

TECHNISCHE UNIVERSITÄT DARMSTADT

Schutzprofil definiert Sicherheitsanforderungen an eine Kategorie von Produkten

- **Smart Meter Gateway Protection Profile:** für Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen
- **Security Module Protection Profile:** für Sicherheitsmodul der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen

# BEISPIEL: DIGITALER SPRACHASSISTENT

TECHNISCHE UNIVERSITÄT DARMSTADT

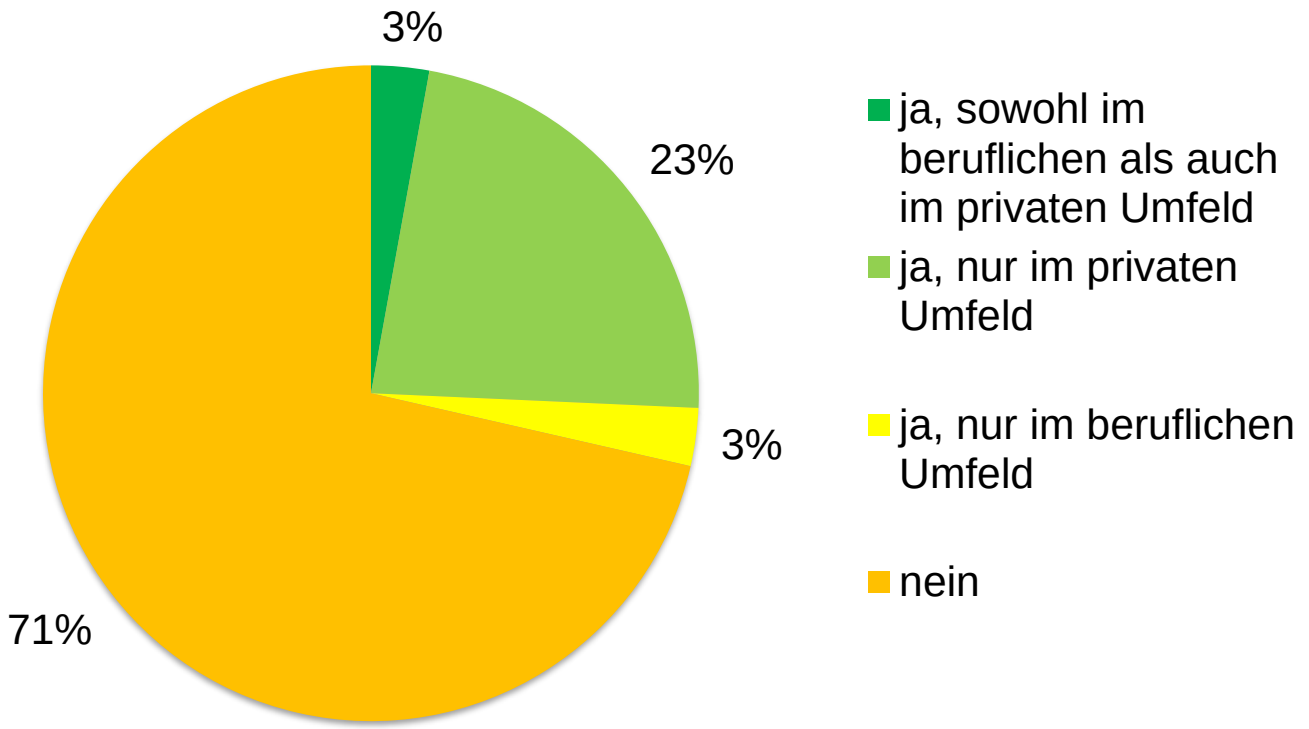
Software, die gesprochene Sprache erkennen, verstehen und sprachgesteuerte Fragen beantworten, Dialoge führen und Assistenzdienste erbringen kann

- Alexa von Amazon, Siri von Apple, Google Assistant von Google, Cortana von Microsoft, Bixby von Samsung, …

Vor allem in Smartphones integriert, aber auch in stationäre Endgeräte, Smart TVs oder Smart Speakers

TECHNISCHE UNIVERSITÄT DARMSTADT

# BENUTZUNG DIGITALER SPRACHASSISTENTEN




»BIOMETRISCHE ERKENNUNGSSYSTEME – NUTZEN UND HEMMNISSE IM VERBRAUCHERALLTAG«, STUDIE DES DIN-VERBRAUCHERRATS, 2020

# BEISPIEL: GOOGLE HOME

TECHNISCHE UNIVERSITÄT DARMSTADT

- mit Hilfe von Sprachbefehlen steuerbarer Lautsprecher mit drahtloser Verbindung zum Internet
- von einer Stimme aus einem Werbespot missbraucht, um einen anpreiserischen Wikipedia-Eintrag akustisch auszugeben [https://www.youtube.com/embed/n5lj63-nc5g]
- Benutzer waren nicht begeistert
- Hinzufügung von Sprecher-Erkennung, um unbefugte Benutzung vorzubeugen und personalisierte Dienste zu ermögliche.


April 12, 2017
1:49 pm EDT

By Mary Beth Quirk
@marybethquirk

ADVERTISING
BADVERTISING
BURGER KING
FAST FOOD
GOOGLE HOME
MARKETING
VOICE ACTIVATED DEVICES
VOICEJACKED

You might think you're the master of your own home, controlling all the internet-connected devices within it and bending them to your will with the touch of a button or an uttered command. But Burger King is trying to sneak into your home through the TV with a new ad that tries to trigger the voice-activated Google Home.

This week, the fast food chain launched a new 15-second TV commercial that attempts to wake up any Google Home devices that may be in the room and thus, continue the ad after it's technically over.

"You're watching a 15-second Burger King ad, which is unfortunately not enough time to explain all the fresh ingredients in the Whopper sandwich," an actor dressed like a Burger King worker says in the spot. "But I got an idea," he adds, uttering Google Home's wake word as the camera gets closer. "OK Google, what is the Whopper burger?"

Burger King hopes that if your device is close enough to the TV, it'll wake up, search the internet, and then spit out a list of its ingredients — whether you want to hear them or not.

# DIGITALER SPRACHASSISTENT

TECHNISCHE UNIVERSITÄT DARMSTADT

- verarbeitet im Bereitschaftsmodus aufgenommene Sprache geräteintern und wartet auf Aufwachbefehl wie „Alexa“, „Hey Siri“, „Ok, Google“

- sendet nach Aufwachbefehl Sprachdaten zur Verarbeitung in die Cloud (auch von Personen, die nicht wissen, dass sie mitgehört werden) – eine geräteinterne Verarbeitung ist aufwendig

- Neue, Datenschutzfreundliche Spracherkennungssoftware belegt nur noch ein halbes Gigabyte Massenspeicher und kann lokal ohne Netzwerkverbindung laufen [https://www.blog.google/products/assistant/next-generation-google-assistant-io/].

TECHNISCHE UNIVERSITÄT DARMSTADT

# EMPFEHLUNGEN ZUM VERBRAUCHER- UND DATENSCHUTZ

formuliert vom 4. rheinland-pfälzischen Verbraucherdialog „Smart Home“ (2016)

[https://mjv.rlp.de/fileadmin/mjv/Themen/Verbraucherschutz/Ergebnispapier_mit_Empfehlungen_zum_Verbraucher__und_Datenschutz_bei_Smart_Home_Angeboten_fuer_Anbieter_sowie_Verbraucherinnen_und_Verbraucher_.pdf]

**1. Installation und Inbetriebnahme:**

- Bei Ersteinrichtung NutzerInnen anhalten, voreingestellte Passwörter zu ändern und Hinweise für sichere Passwörter geben
- Personenbezogene Daten wie Name oder Standort **nur abfragen**, soweit dies für die Nutzung **erforderlich**
- **Anonyme Einrichtung** der verbundene Geräte und Dienste sollte grundsätzlich möglich sein

**2. Geräteeigenschaften:**

- Nach Möglichkeit „Plug & Play“, dabei Sicherheit und Datenschutz beachten
- Fernwartung durch Techniker nur unter Einhaltung **strenger Zugriffskriterien** und nach technischer Freigabe durch den Nutzer **im Einzelfall**

TECHNISCHE UNIVERSITÄT DARMSTADT

# EMPFEHLUNGEN ZUM VERBRAUCHER- UND DATENSCHUTZ

**3. Bedienung:**

- Nutzer sollten gegebenenfalls die Möglichkeit haben, **verschiedene Benutzerkonten** mit unterschiedlichen Berechtigungen zu haben
- Geräte und Dienste müssen einen plötzlichen oder geplanten Stromausfall unbeschadet überstehen können

**5. Interoperabilität und Erweiterbarkeit**

- Geräte und Dienste sollten auf der Grundlage von offenen oder mit einer Vielzahl von Anbietern gemeinsam entwickelten Standards und Schnittstellen miteinander kommunizieren, **soweit dies die Sicherheit nicht beeinträchtigt.**

**6. Haltbarkeit**

- Anbieter sollten Geräte und Dienste über eine möglichst lange Zeit hinweg unterstützen. Dazu gehören insbesondere technische Hilfe und die **Bereitstellung von Sicherheitsupdates**

TECHNISCHE UNIVERSITÄT DARMSTADT

# EMPFEHLUNGEN ZUM VERBRAUCHER- UND DATENSCHUTZ

## 7. Personenbezug und grundsätzliche Zweckbindung von Daten

- Anbieter und Hersteller von Smart Home-Lösungen haben zu berücksichtigten, dass es sich bei den anfallenden Daten in der Regel um **personenbezogene, jedenfalls personenbeziehbare Daten** handelt. Soweit bei rein technischen Daten (z.B. Sensorwerte) durch Verknüpfung mit weiteren Informationen ein Bezug zum jeweiligen Nutzer beziehungsweise Vertragspartner hergestellt werden kann, **ergibt sich auch hier ein Personenbezug**. Dieser Personenbezug ist dabei unabhängig von der gegebenenfalls unterschiedlichen Sensitivität einzelner Datenkategorien.
- Die Verwendung personenbezogener Daten ist nur zulässig, soweit dies eine Rechtvorschrift erlaubt oder der Betroffene eingewilligt hat. Die Einwilligung muss insbesondere freiwillig und informiert erfolgen.
- Danach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.
- Neben den Nutzerinnen und Nutzern können dies zum Beispiel Anbieter, Hersteller, aber auch weitere eingebundene Dienstleister sein.

TECHNISCHE UNIVERSITÄT DARMSTADT

# EMPFEHLUNGEN ZUM VERBRAUCHER- UND DATENSCHUTZ

**7. Personenbezug und grundsätzliche Zweckbindung von Daten**

- Dem Grundsatz der Zweckbindung entsprechend dürfen personenbezogene Daten nur zu dem **Zweck** verwendet werden, zu dem sie **ursprünglich erhoben wurden**. Eine darüber hinaus gehende zweckändernde Verwendung personenbezogener Daten, zum Beispiel zu Marketingzwecken, bedarf daher einer gesonderten datenschutzrechtlichen Rechtfertigung. Dies wird in der Regel nur im **Wege der Einwilligung** möglich sein.

**8. Transparenz der Datenverwendung**

- Zum effektiven Schutz des informationellen Selbstbestimmungsrechts von Nutzerinnen und Nutzern haben Hersteller und Anbieter von Smart Home-Anwendungen sicherzustellen, dass die stattfindenden **Datenflüsse transparent und nachvollziehbar** sind. Nur so werden die Betroffenen in die Lage versetzt, eine verantwortliche Entscheidung über die Nutzung einzelner Anwendungen zu treffen

TECHNISCHE UNIVERSITÄT DARMSTADT

# EMPFEHLUNGEN ZUM VERBRAUCHER- UND DATENSCHUTZ

## 8. Transparenz der Datenverwendung

- **Grundsatz der Transparenz:**
  - Welche Daten auf welcher Rechtsgrundlage, in welchem Umfang, in welcher Weise und zu welchem Zweck verarbeitet werden
  - Welche Daten zur Erfüllung des Vertragszwecks erforderlich sind und welche gegebenenfalls zu anderen Zwecken erhoben werden
  - Wer für einzelne Datenverarbeitungsprozesse verantwortlich ist. Das gilt insbesondere auch bei der Einbindung Dritter. Soweit Dienstleister einbezogen werden, die für die Erfüllung des Vertragszweckes von wesentlicher Bedeutung sind, sollten die Nutzerinnen und Nutzer darüber informiert werden.
  - Ob und in welchem Umfang Nutzerinnen und Nutzer die Möglichkeit haben, selbst Einfluss auf einzelne Datenverarbeitungsprozesse zu nehmen.
  - Wie Nutzerinnen und Nutzer effektiv ihre Betroffenenrechte ausüben können (Auskunfts-, Berichtigungs- und Löschungsansprüche

TECHNISCHE UNIVERSITÄT DARMSTADT

# EMPFEHLUNGEN ZUM VERBRAUCHER- UND DATENSCHUTZ

## 9. Datensouveränität

- Die Verarbeitung personenbezogener Daten der Betroffenen darf nur unter deren Kontrolle erfolgen.
- Soweit externe Zugriffe, zum Beispiel im Rahmen einer **Fernwartung**, auf Smart Home-Anwendungen erforderlich sind, ist festzulegen, wie Nutzerinnen und Nutzer diese **erkennen** und unter welchen Voraussetzungen sie diese **unterbinden können**. Nutzerinnen und Nutzer haben das Recht, die Datenflüsse aus ihrem häuslichen Bereich zu unterbinden, unbeschadet vertraglicher Pflichten.
- Im Falle eines Besitzwechsels der Smart Home-Lösung oder Beendigung des Vertragsverhältnisses muss sichergestellt sein, dass Nutzerinnen und Nutzer ihre **personenbezogenen Daten löschen** können.

## 10. Datensparsamkeit

- Bei der Gestaltung von Smart Home-Lösungen sollte darauf geachtet werden, dass anfallende Daten möglichst ohne (direkten) Personenbezug verarbeitet werden. Dies gilt insbesondere dann, wenn die Daten außerhalb des häuslichen Bereichs verarbeitet werden
- Insbesondere bei Geräte-, Verbrauchs- und Nutzungsdaten ist **ein Personenbezug häufig nicht erforderlich**. Anbieter und Hersteller sollten daher bereits bei der Entwicklung ihrer Lösungen auf die Verarbeitung der Daten in personenbezogener Form verzichten, wenn dies für die Funktionalität nicht benötigt wird

TECHNISCHE UNIVERSITÄT DARMSTADT

# EMPFEHLUNGEN ZUM VERBRAUCHER- UND DATENSCHUTZ

## 10. Datensparsamkeit

- Wenn Zusatzfunktionen oder Mehrwertdienste eine Personenbeziehbarkeit voraussetzen, sollte den Nutzerinnen und Nutzern eine Wahlmöglichkeit angeboten werden. Die **Voreinstellungen** sollten dabei auf eine **datensparsame beziehungsweise pseudonyme Verarbeitung** der im Rahmen der Smart Home-Lösung anfallenden Daten ausgelegt sein, so dass Änderungen bewusst vorgenommen werden müssen.
- Wo aus Gründen der Funktionalität eine individuelle Zuordnung zum Beispiel von Geräte-, Verbrauchs- oder Nutzungsdaten zu bestimmten Personen unerlässlich ist, sollten **pseudonyme Verarbeitungsmöglichkeiten** vorgesehen werden.

TECHNISCHE UNIVERSITÄT DARMSTADT

# EMPFEHLUNGEN ZUM VERBRAUCHER- UND DATENSCHUTZ

## 11. Kontroll- und Steuerungsmöglichkeiten für NutzerInnen

- Möglichkeiten vorsehen, die es den NutzerInnen erlaubt, den gewünschten Funktionsumfang beziehungsweise Art und **Umfang der verarbeiteten Daten selbst festzulegen** und gegebenenfalls zu ändern.
- Möglichkeiten für **eine Einsichtnahme** der Nutzerinnen und Nutzer in die gespeicherten Daten vorhanden sein
- Möglichkeiten **zur Löschung** von Geräte-, Verbrauchs- und Nutzungsdaten durch die Nutzerinnen und Nutzer vorhanden sein.
- **Benutzeranmeldungen, Zugriffe auf Geräte-, Verbrauchs- und Nutzungsdaten, Datenübertragungen an Stellen** außerhalb des häuslichen Bereichs und die Änderung von Systemeinstellungen sollten anhand einer geeigneten, manipulationssicheren **Protokollierung** nachvollzogen werden können.

TECHNISCHE UNIVERSITÄT DARMSTADT

# EMPFEHLUNGEN ZUM VERBRAUCHER- UND DATENSCHUTZ

**12. Sicherheit bei Datenspeicherung, Übertragung und –zugriff**

- alle Übertragungen personenbezogener Daten, d.h. innerhalb des häuslichen Umfeldes sowie bei der Übertragung an externe Stellen, **nur über verschlüsselte Verbindungen** erfolgen
- sollten auf den Systemen der Anbieter/Hersteller sowie gegebenenfalls einbezogener weiterer Stellen nur in **verschlüsselter Form** gespeichert werden.
- Datenzugriffe sowie die Änderung von System- und Benutzereinstellungen dürfen nur auf der Grundlage einer **verlässlichen Authentifizierung** der Benutzer beziehungsweise beteiligter Komponenten möglich sein.

TECHNISCHE UNIVERSITÄT DARMSTADT

KAPITEL 5

# LERNZIELE

© Thomas Ott

TECHNISCHE UNIVERSITÄT DARMSTADT

# LERNZIELE

- Sie wissen, was personenbezogene Daten sind und unter welchen Bedingungen diese verarbeitet werden dürfen
- Sie können Datenschutzprobleme von AmI-Systemen aufzeigen und bewerten