„DAS VERMESSENE ICH“

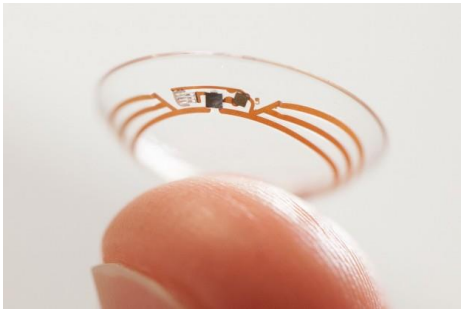
WEARABLE COMPUTING AUS DATENSCHUTZRECHTLICHER SICHT

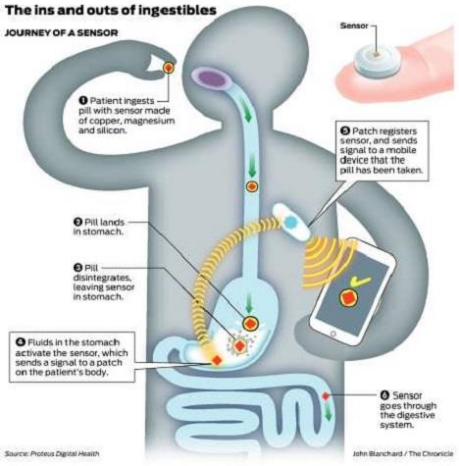
JOHANNES KEPLER
UNIVERSITÄT LINZ

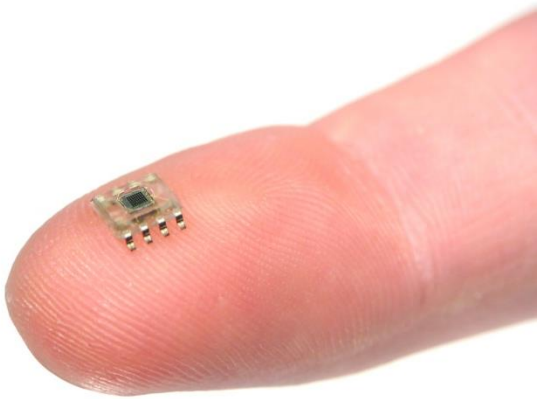
WEARABLE COMPUTING DEVICES („WEARABLES“)

- Computersysteme, die dafür konzipiert sind, im oder am Körper getragen zu werden
- Integrierte Sensoren mittels denen Daten der Umwelt und des Trägers ermittelt werden
- Digitale Schnittstelle nach außen (beispielsweise Bluetooth oder WLAN)
- Neue Form der Mensch-Maschine-Interaktion
- Unterstützung des Nutzers
- Keine Beeinträchtigung der Aufmerksamkeit oder Mobilität des Nutzers

ANWENDUNGSFELDER







DATENSCHUTZZIELE

- Schutz der Privatsphäre des Menschen vor den Gefahren, die durch die Möglichkeit von Auswertungen und Verknüpfungen elektronisch verfügbarer Daten entstehen
- Angemessener Ausgleich zwischen der Datenverarbeitung und dem Schutz der Betroffenen

DATENSCHUTZ ALS GRUNDRECHT

- Grundrechte = verfassungsgesetzlich gewährleistete Rechte
- § 1 DSG (bis und ab 25. Mai 2018) = Verfassungsbestimmung
- **Grundrecht auf Datenschutz**
  - Recht auf Geheimhaltung personenbezogener Daten
  - Recht auf Auskunft über die Verwendung personenbezogener Daten
  - Recht auf Richtigstellung falscher Daten
  - Recht auf Löschung unrechtmäßig verarbeiteter Daten

DIREKTE ANWENDBARKEIT DER DSGVO

ab 25. Mai 2018

Aktuell:

Datenschutz-
Richtlinie

Umsetzung

Datenschutzgesetz
DSG 2000

Zukünftig:

Datenschutz-
Grundverordnung

Direkt anwendbar

Aber:
Öffnungsklauseln

Datenschutzgesetz
(Datenschutz-
Anpassungsgesetz
2018)

JKU

SACHLICHER ANWENDUNGSBEREICH (I)

- Art 2 DSGVO
- Elektronisch verarbeitete Daten
- Manuell verarbeitete Daten → Dateisystem

Hinweis
Eine nach Namen geordnete Personalaktenverwaltung in Papierform wird die Kriterien eines Dateisystems erfüllen. Anwendbarkeit der DSGVO.

SACHLICHER ANWENDUNGSBEREICH (II)

Ausnahmen (ua):

- „Haushaltsausnahme“

Hinweis
Die private Nutzung sozialer Netzwerke oder die Erfassung von Kontaktdaten am privaten Handy fallen aufgrund des privaten Anwendungsbereichs nicht unter die DSGVO.

- Anonyme Daten

PERSONENBEZOGENE DATEN (I)

- Art 4 Z 1 DSGVO
- „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“
- Informationen = sämtliche Arten von Aussagen
- Materielle Aussage muss sich auf eine natürliche Person beziehen, die das Informationsobjekt des Datums darstellt
- Objektbezogene Informationen = personenbezogene Daten?
  - Beschreibung einer Personen-Sach-Beziehung
  - Aussage über Eigentums-, Besitz- oder Nutzungsrechten an einem Objekt
  - Mittelbare Personeninformation

PERSONENBEZOGENE DATEN (II)

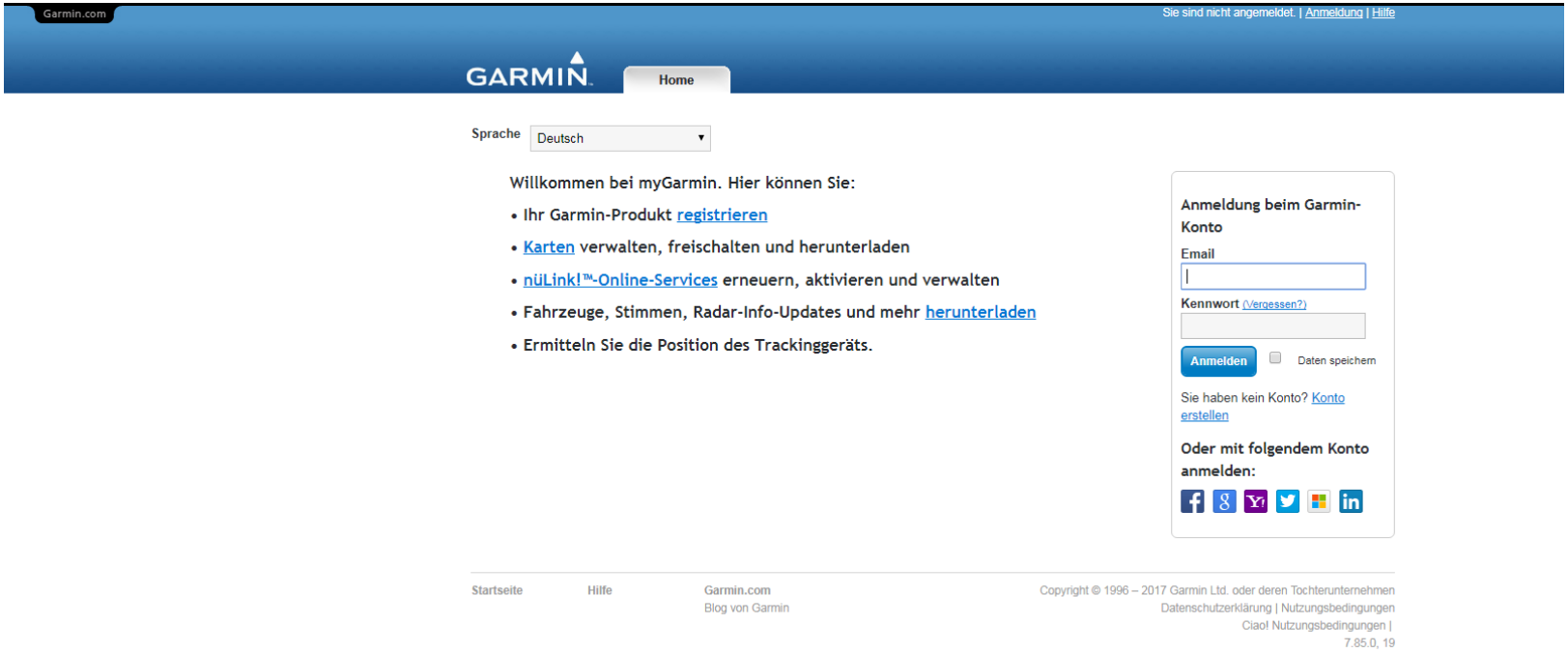
- Der hinter einer konkreten Information Stehende muss mit ihrer Hilfe identifiziert oder zumindest identifizierbar sein
- Fixierung in einer verarbeitbaren Form
- Besondere Kategorien personenbezogener Daten („sensible Daten“) → strengere Maßstäbe
- Gesundheitsdaten = alle Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen

Beispiele
Name, Adresse, Geburtsdatum, KFZ-Kennzeichen, Sozialversicherungsnummer, Bankkonto, Standortdaten

JKU

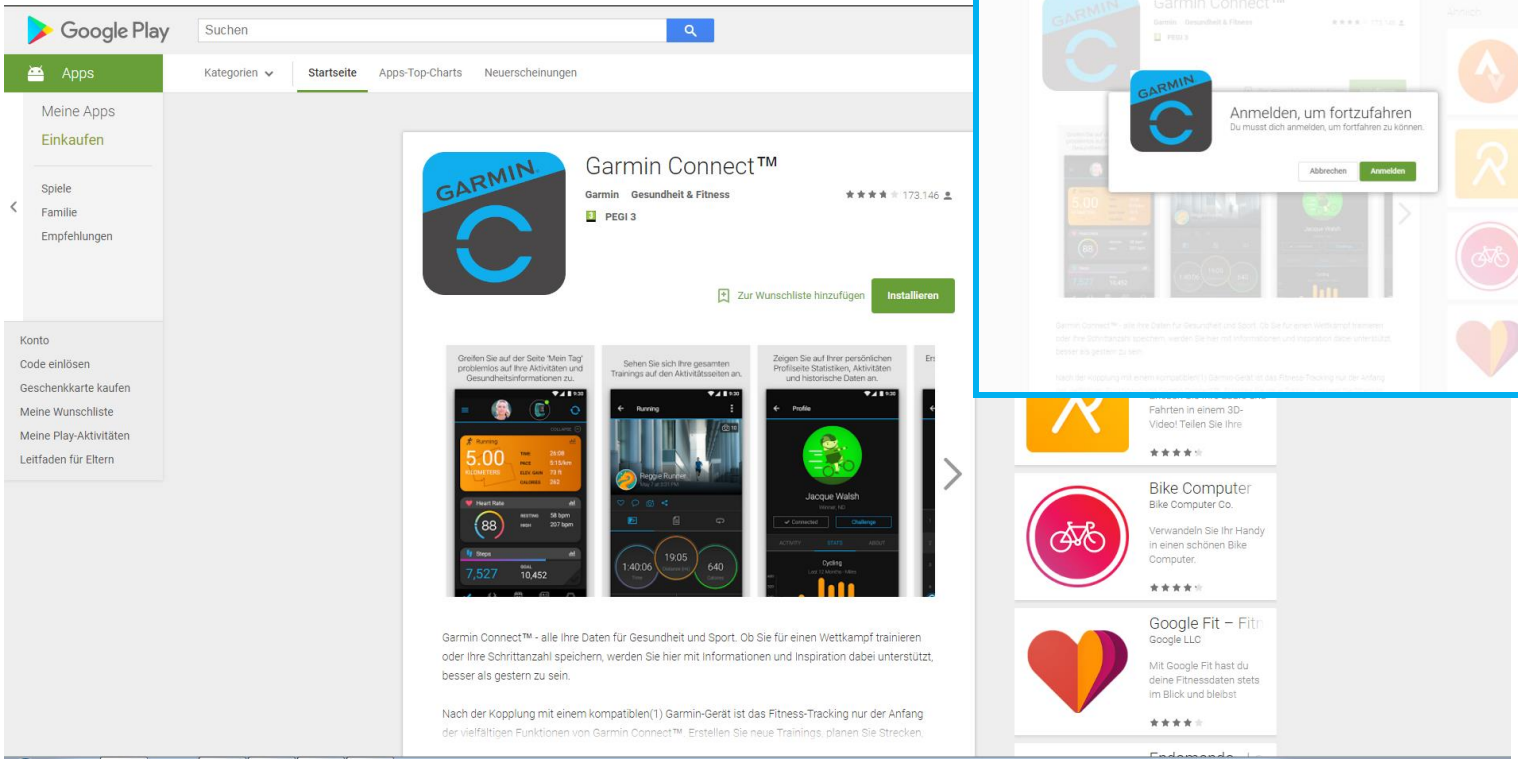
KLASSIFIZIERUNG DER DATEN EINER WEARABLE-ANWENDUNG (I)

- Einrichtung eines Benutzerkontos



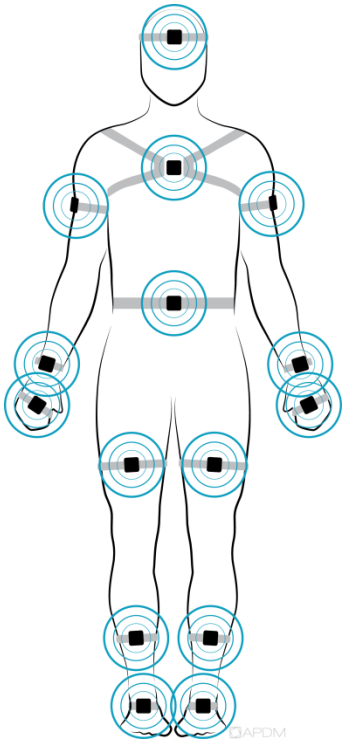
KLASSIFIZIERUNG DER DATEN EINER WEARABLE-ANWENDUNG (II)

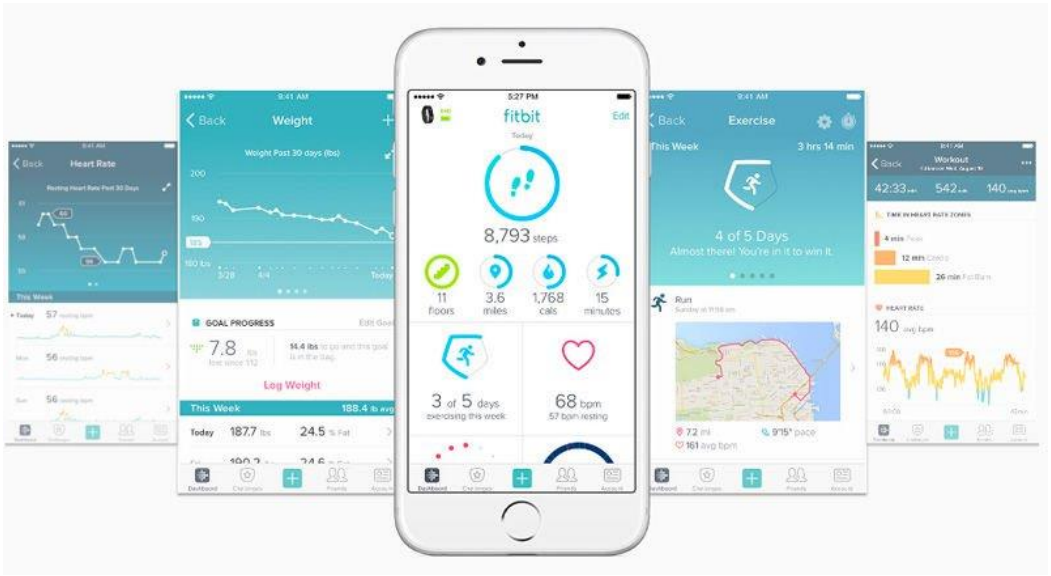
- Bezug der notwendigen App



KLASSIFIZIERUNG DER DATEN EINER WEARABLE-ANWENDUNG (III)

- Erhebung und Visualisierung der Rohdaten





JKU

PSEUDONYMISIERTE DATEN

- Daten sind grundsätzlich noch einer bestimmten Person zuordenbar **ABER**
- Zuordnung ist nur mit zusätzlichen Informationen möglich
- Ausreichende technische und organisatorische Maßnahmen wurden getroffen, damit diese Zuordnung nicht (mehr) erfolgt

Hinweis
Anwendbarkeit der DSGVO

JKU

ANONYME DATEN

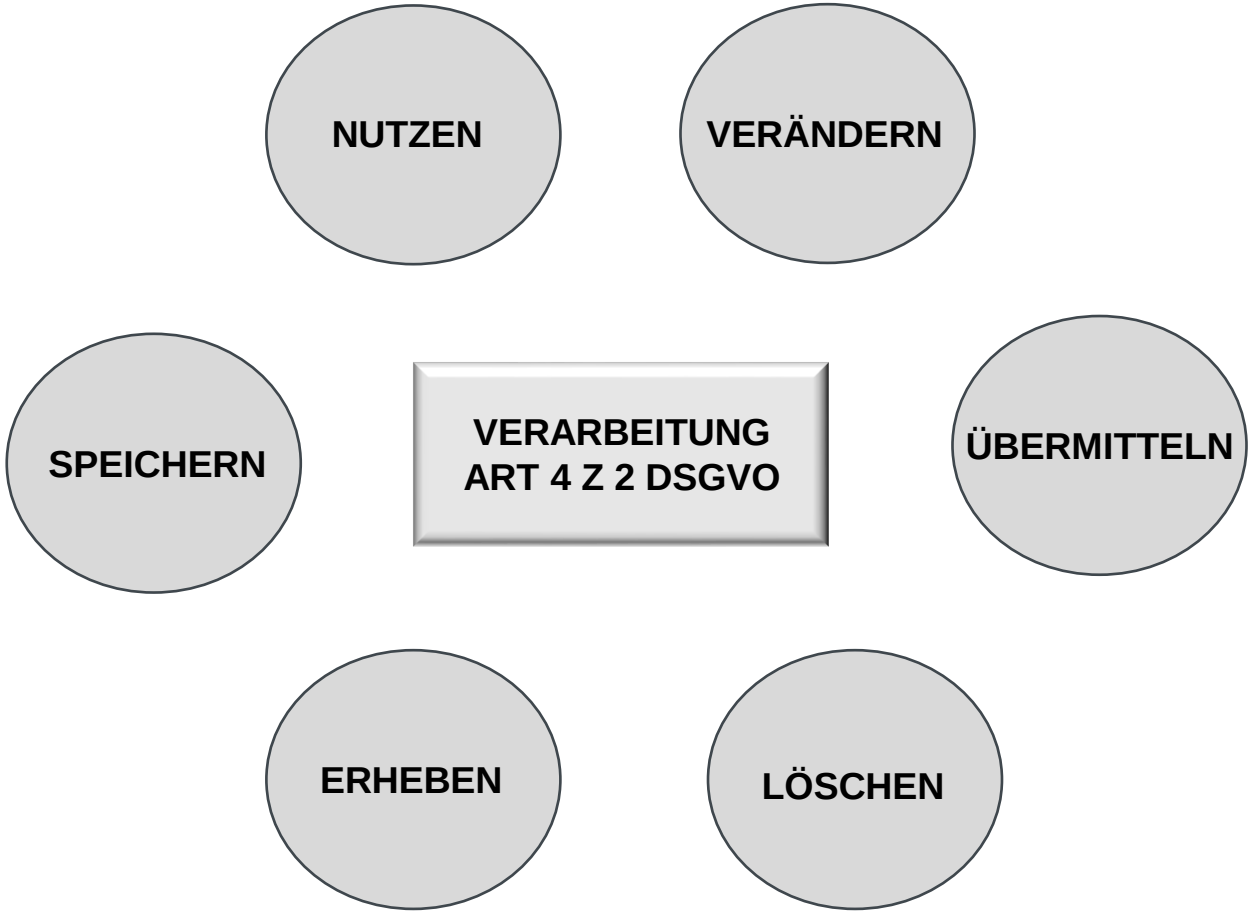
- Anonym = nicht mehr personenbezogen
- Daten können von niemanden mehr einer natürlichen Person zugeordnet werden
- Die Zuordnung ist nicht nur durch technische und organisatorische Mittel erschwert, sondern unmöglich
- Unmöglichkeit = wenn die Zuordnung zwar technisch noch möglich ist, aber mit einer Zuordnung nicht zu rechnen ist (insb in Anbetracht des benötigten Zeit- und Kostenaufwands)

Hinweis
Keine Anwendbarkeit der DSGVO

PSEUDONYMISIERTE DATEN ODER ANONYME DATEN?

- Getrennte Speicherung der Wearable-Daten von den Identifikationsdaten, damit kein Rückschluss von den Daten eines Geräts auf den Probanden erfolgen kann
- Keine Anonymisierung!! Sondern **Pseudonymisierung**
- Zwei getrennte Datenbanken
- Die Daten des Probanden referenzieren sich wechselseitig über einen gemeinsamen Probandenidentifikator (ID)
- Pseudonymisierungen heben den Personenbezug nicht auf, sondern stellen Maßnahmen der Datensparsamkeit und Datensicherheit dar

VERARBEITUNG (I)



VERARBEITUNG (II)

- Erhebung von Identifikationsdaten
- Speicherung der durch das Wearable aufgezeichneten Rohdaten
- Anschließende Nutzung der durch das Wearable aufgezeichneten Rohdaten

ROLLENVERTEILUNG (I)

Betroffener

Personen, deren Daten verarbeitet werden und auf die sich die verarbeiteten Daten beziehen

= Schutzsubjekt

Verantwortlicher

natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet

Weisung

Auftragsverarbeiter

natürliche oder juristische Person, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet

JKU

ROLLENVERTEILUNG (II)

Betroffener

Personen, deren Daten verarbeitet werden und auf die sich die verarbeiteten Daten beziehen

- **Wearable-Nutzer**
- **Aber auch Nichtnutzer („intelligente Brille“)**

Verantwortlicher

natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet

- **Wearable-Hersteller**
- **App-Anbieter (-Entwickler)**
- **App-Store-Betreiber**
- **Sonstige Dritte**

JKU

RÄUMLICHER ANWENDUNGSBEREICH (I)

- Art 3 DSGVO
- Datenverarbeitung erfolgt im Rahmen der Tätigkeiten einer Niederlassung in der Union
- Unerheblich, ob die Verarbeitung in der Union stattfindet
- Niederlassung = effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung

Beispiel
Die Kundendaten eines österreichischen Handelsunternehmens werden vom Mutterkonzern in den USA gespeichert.

RÄUMLICHER ANWENDUNGSBEREICH (II)

- Niederlassung außerhalb der EU
- „Marktortprinzip“

Beispiel
Ein US-Unternehmen bietet über das Internet Bücher in Österreich an.

Beispiel
Ein kanadisches Unternehmen beobachtet mithilfe eines Analysetools das Einkaufverhalten von Österreichern.

GRUNDSÄTZE

- Art 5 Abs 1 DSGVO
- Rechenschaftspflicht (Art 5 Abs 2 DSGVO)
- Der Verantwortliche ist für die Einhaltung der Grundsätze verantwortlich und muss deren Einhaltung nachweisen können

Sanktion: bis zu 20 Mio Euro oder 4 % des letztjährigen weltweiten Jahresumsatzes

RECHTMÄßIGKEIT, VERARBEITUNG NACH TREU UND GLAUBE, TRANSPARENZ

- Art 5 Abs 1 lit a DSGVO
- Datenverarbeitung aufgrund einer Einwilligung oder einer sonstigen zulässigen Rechtsgrundlage
- Datenverarbeitung niemals ohne Kenntnis des Betroffenen
- Datenverarbeitung in nachvollziehbarer Weise
  - Informationen und Mitteilungen leicht zugänglich und verständlich
  - In klarer und einfacher Sprache abgefasst

ZWECKBINDUNGSGRUNDSATZ

- Art 5 Abs 1 lit b DSGVO
- Daten dürfen nur für **festgelegte**, **eindeutige** und **legitime** Zwecke erhoben werden
- Verwendung bestehender Datenbestände für neue Zwecke problematisch → Vereinbarkeit mit dem Erhebungszweck?

Hinweis
Datenbesitz legitimiert nicht zur unbeschränkten Datenverwendung.

JKU

DATENMINIMIERUNG

- Art 5 Abs 1 lit c DSGVO
- Art und Umfang der verarbeiteten Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung **notwendige Maß** beschränkt sein

Hinweis
Wenn das Alter einer Person relevant ist, ist es nicht notwendig, ihr Geburtsdatum zu speichern.

GRUNDSATZ DER RICHTIGKEIT

- Art 5 Abs 1 lit d DSGVO
- Es sollen nur sachlich richtige Daten verarbeitet werden
- Unrichtige Daten sind unverzüglich zu löschen bzw zu berichtigen

GRUNDSATZ DER SPEICHERBEGRENZUNG

- Art 5 Abs 1 lit e DSGVO
- Daten dürfen nicht länger als für die Zweckerreichung nötig gespeichert werden
- Beschränkung der Speicherfrist auf das unbedingt erforderliche Mindestmaß
- Fristen für die Löschung oder regelmäßige Überprüfungen vorsehen

INTEGRITÄT UND VERTRAULICHKEIT

- Art 5 Abs 1 lit f DSGVO
- Verarbeitung der personenbezogenen Daten in einer Weise, die eine angemessene Sicherheit gewährleistet
- Kein Zugang zu den Daten für Unbefugte

RECHTE DER BETROFFENEN

- Informationsrecht
- Auskunftsrecht
- Berichtigungsrecht
- Recht auf Löschung
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht

Sanktion: bis zu 20 Mio Euro oder 4 % des letztjährigen weltweiten Jahresumsatzes

JKU

DATENSICHERHEITSMAßNAHMEN

- Implementierung angemessener Datensicherheitsmaßnahmen
- Meldung gewisser Sicherheitsverletzungen
- **Maßnahmen**
  - ☐ Pseudonymisierung und Verschlüsselung personenbezogener Daten
  - ☐ Maßnahmen zur Sicherung der IT-Systeme
  - ☐ Datenwiederherstellungsprozess
  - ☐ Regelmäßige Überprüfung der Sicherheitsmaßnahmen

Sanktion: bis zu 10 Mio Euro oder 2 % des letztjährigen weltweiten Jahresumsatzes

DATENVERARBEITUNG ZULÄSSIG (I)

- Grundsätzliches Verbot der Datenverarbeitung
- Taxativ aufgezählte Erlaubnistatbestände
- Art 6 DSGVO bzw für „sensible“ Daten Art 9 DSGVO

Hinweis
Prinzip des Verbots mit Erlaubnisvorbehalt

DATENVERARBEITUNG ZULÄSSIG (II)

- Einwilligung als zentrale Legitimationsform
- Art 6 Abs 1 lit a DSGVO bzw Art 9 Abs 1 lit a DSGVO
- (Gültige) Einwilligung = eine
  - freiwillig,
  - für den bestimmten Fall,
  - in informierter Weise,
  - unmissverständlich und, bei „sensiblen“ Daten, ausdrücklich abgegebene
  - Willensbekundung

DATENVERARBEITUNG ZULÄSSIG (III)

Einwilligung bei Wearable-Anwendungen

- Freiwilligkeit gegeben?
  - Wearable-Nutzer hat die zumutbare Möglichkeit, ein anderes Produkt zu verwenden oder auf die Nutzung gänzlich zu verzichten
  - Wearables und Fitness-Apps als digitales Bonusheft
  - Vorliegen einer realistischen Entscheidungsmöglichkeit
- Bestimmtheit der Einwilligung?

FORSCHUNGSPRIVILEG

- Art 5, 9 und 89 DSGVO
- Weiterverarbeitung von Daten für wissenschaftliche Forschung nicht unvereinbar mit dem Erhebungszweck
- Längere Speicherung möglich
- Verarbeitung der Daten in anonymisierter bzw pseudonymisierter Form
- Allgemein gehaltene Zustimmungserklärung
- Ausnahmsweise Verarbeitung sensibler Daten ohne Einwilligung → Öffnungsklausel (Art 9 Abs 2 lit j DSGVO)

BEHÖRDE

- Einrichtung einer Datenschutz-Aufsichtsbehörde
- **Befugnisse**
  - Untersuchungsbefugnisse
  - Abhilfebefugnisse (zB Verwarnung, Anweisung, Anordnung der Beschränkung der Datenverarbeitung, der Berichtigung oder der Löschung von Daten, Verhängung von Geldbußen)
  - Beratungs- und Genehmigungsbefugnisse
- Österreich: Datenschutzbehörde

JOHANNES KEPLER
UNIVERSITÄT LINZ

VIELEN DANK

Univ.-Ass. Mag. Sarah Heiml
Institut für Verwaltungsrecht und Verwaltungslehre
Abteilung Technikrecht

JOHANNES KEPLER
UNIVERSITÄT LINZ
Altenberger Straße 69
4040 Linz, Österreich
www.jku.at