Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik

Künstliche Intelligenz im Spannungsfeld von Datenschutz

Prof. Ursula Sury
Hochschule Luzern – Informatik: Vizedirektorin Weiterbildung

T direkt +41 41 757 68 52
Ursula.sury@hslu.ch

Rotkreuz 04.12.2019

Luzerner Kongress Gesellschaftspolitik 2019

Agenda

1. Künstliche Intelligenz (KI)
2. Datenschutz
3. Spannungsfeld

1. Künstliche Intelligenz (KI)

Definition Künstliche Intelligenz

- Künstliche Intelligenz bezeichnet Maschinen, die menschliche kognitive Fertigkeiten wie das Lösen von Problemen oder andere Fähigkeiten nachahmen, die Sprache, Sprechen und strategisches Denken voraussetzen.
- KI-Anwendungen versetzen Maschinen in die Lage, bestimmte menschliche Aufgaben genauso gut oder sogar besser auszuführen.

Merkmale:

Künstliche Intelligenz (KI) versetzt

- Maschinen in die Lage, aus Erfahrung zu lernen,
- sich auf neu eingehende Information einzustellen
- und Aufgaben zu bewältigen, die menschenähnliches Denkvermögen erfordern.

Die meisten heute geläufigen Beispiele für (KI)

- von Schach spielenden Computern
- bis hin zu selbstfahrenden Autos –
- basieren vor allem auf Deep Learning und natürlicher Sprachverarbeitung.
- Mit diesen Technologien können Computer für ganz bestimmte Aufgaben trainiert werden, indem sie große Datenmengen verarbeiten und in diesen Daten Muster erkennen.

Maschinelles Lernen (ML)

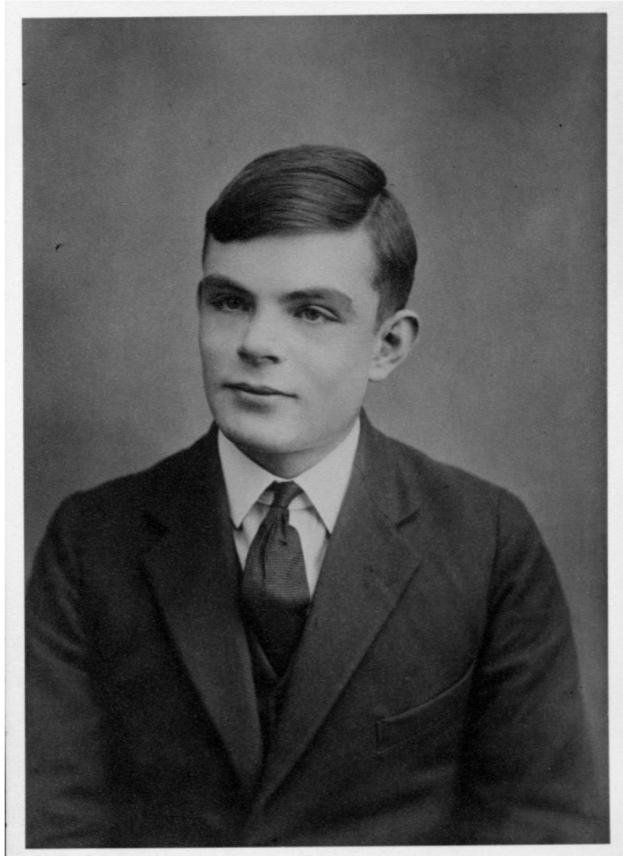
Maschinelles Lernen ist ein Teilbereich der Künstlichen Intelligenz. Zwei Erkenntnisse haben ML vorangetrieben:

- die Vorstellung, dass Maschinen das Lernen lernen können und das Internet.
- Maschinen etwas beizubringen, ist ein mühsames Unterfangen.
- Wenn man ihnen jedoch Zugang zur grenzenlosen Datenfülle des Internets verschafft, können sie selbst lernen - und das hat zahllose neue Perspektiven eröffnet.

Alan Turing

Alan Mathison Turing OBE (* 23. Juni 1912 in London; † 7. Juni 1954 in Wilmslow, Cheshire)

- **war ein britischer Logiker, Mathematiker, Kryptoanalytiker und Informatiker.**
- **er gilt heute als einer der einflussreichsten Theoretiker der frühen Computerentwicklung und Informatik.**
- **Turing schuf einen großen Teil der theoretischen Grundlagen für die moderne Informations- und Computertechnologie.**

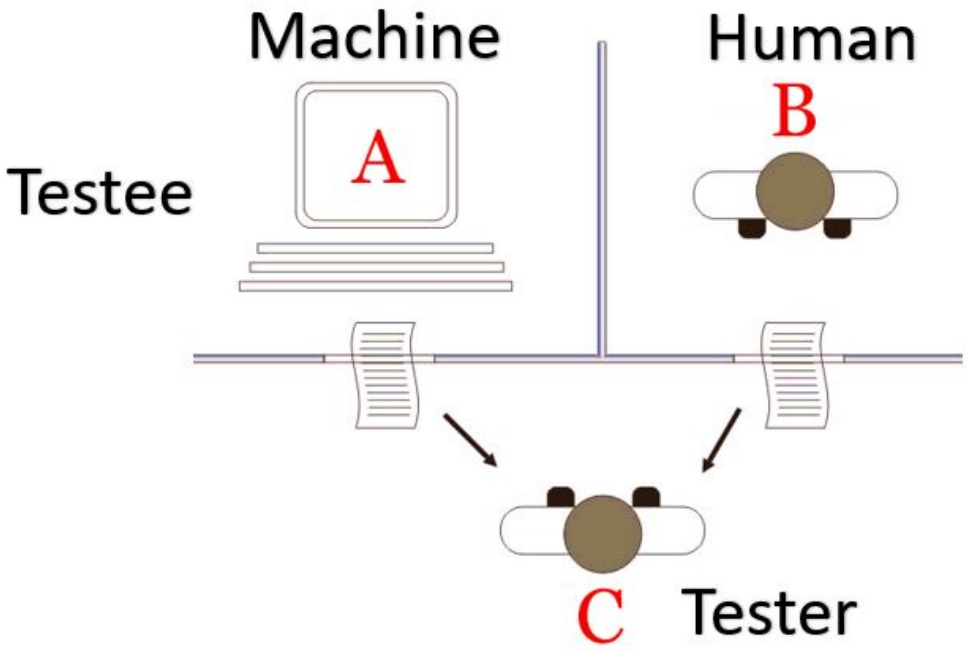


Turing Test

Turing Test:

- Mit dem später sogenannten Turing-Test formulierte Alan Turing im Jahr 1950 eine Idee, wie man feststellen könnte, ob ein Computer, also eine Maschine, ein dem Menschen gleichwertiges Denkvermögen hätte. Dieser Test war zunächst nur eine theoretische Skizze.

- Sie wurde erst später genauer und konkreter ausformuliert nachdem die künstliche Intelligenz als Teilbereich der Informatik, zu einem eigenständigen akademischen Fachgebiet geworden war.



Chinese Room

- **Das Chinesische Zimmer ist der Name für ein Gedankenexperiment des Philosophen John Searle.**
- **Mit seiner Hilfe versucht Searle die Meinung zu widerlegen, dass digitale Computer allein dadurch Bewusstsein erlangen könnten, dass sie ein passendes Programm ausführen**
- **Bei dem Gedankenexperiment stellt man sich einen geschlossenen Raum vor, in dem ein Mensch, der keinerlei Chinesisch versteht, in chinesischer Schrift gestellte Fragen – anhand einer in seiner Muttersprache verfassten Anleitung – in chinesischer Schrift sinnvoll beantwortet. Personen außerhalb des Raums folgern aus den Ergebnissen, dass der Mensch in dem Raum Chinesisch beherrscht, obwohl das nicht der Fall ist**
- **Das Experiment sollte zeigen, dass ein Computer ein Programm ausführen und regelbasiert Zeichenreihen verändern kann, ohne die Bedeutung der Zeichen zu verstehen**

Artificial Intelligence vs. Cognitive Science

Build Intelligent Software Systems

- algorithms to achieve intelligent behavior
- problems that only humans can solve are solved by computers
- do not mimic/replicate human intelligence

➢ part of computer science, links to mathematics, economics

Understand Human Intelligence

- what constitutes (human) intelligence?
- how do people solve problems?
- build models of human intelligence/the brain

➢ part of neuro & brain sciences, links to psychology

Modelle und Algorithmen – 3 Arten von Systemen

Training
Verallgemeinerung von Beispielen
via statistische Mustererkennung
Maschinelles Lernen

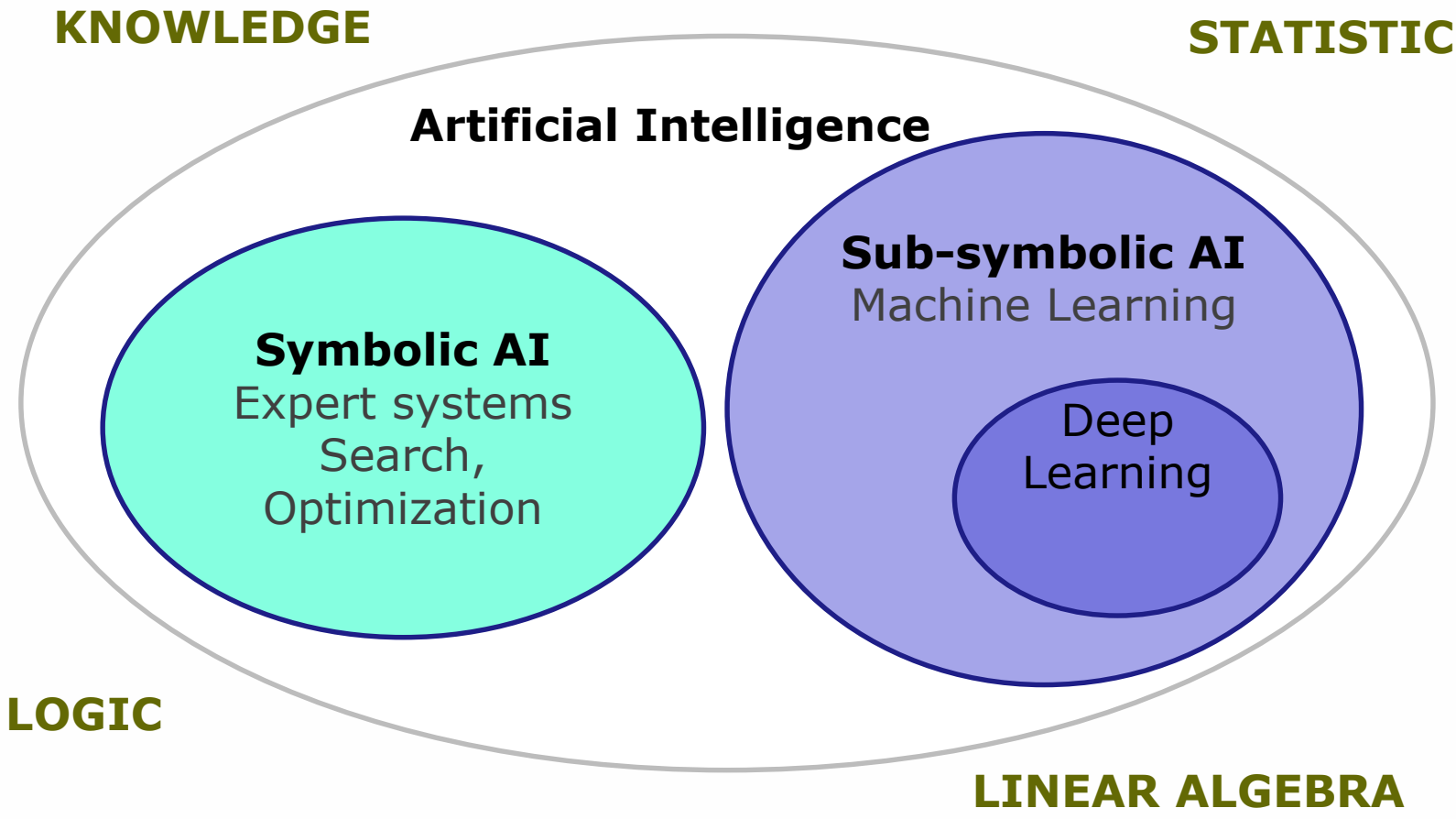
Exploration
Erfahrung sammeln durch Aktionen
& Feedback
Reinforcement Learning

Engineering
Menschliches Wissen und Erfahrung
in formale Modelle übertragen
Solver

+

=

intelligentes Verhalten in den modellierten Situationen und Anwendungs-problemen
(und NUR dort!)

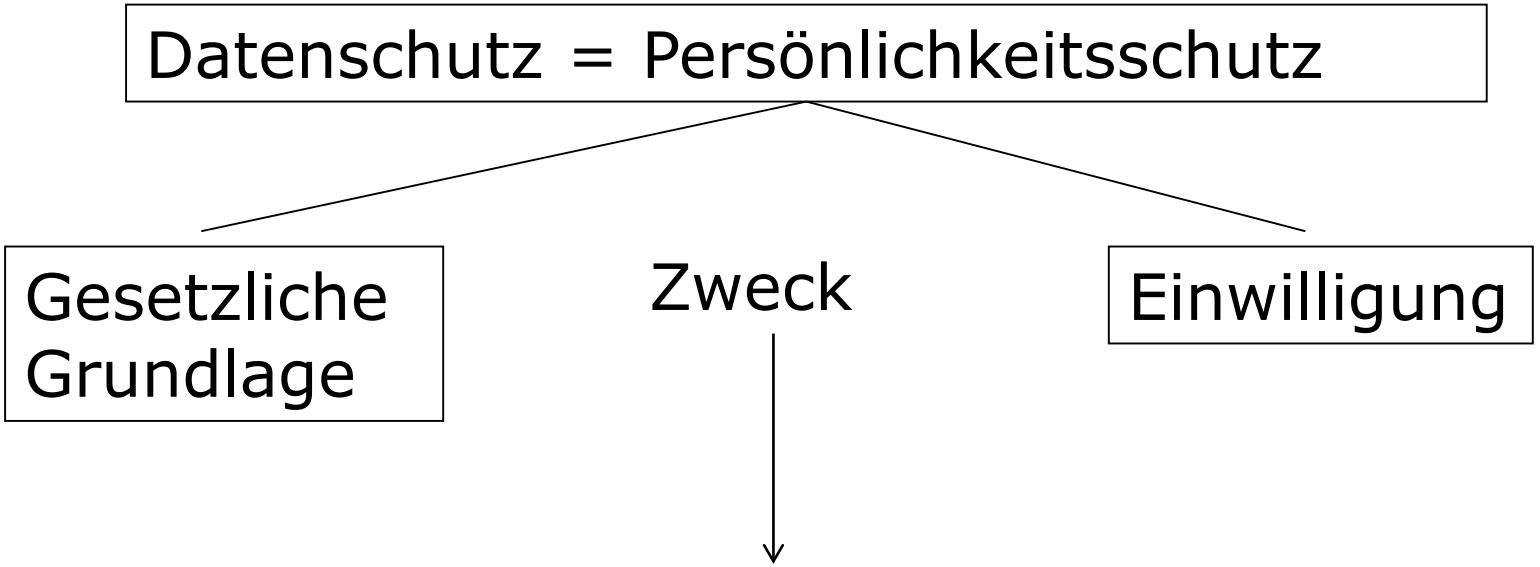

KNOWLEDGE
STATISTICS
Artificial Intelligence
Symbolic AI
Expert systems
Search,
Optimization
Sub-symbolic AI
Machine Learning
Deep
Learning
LOGIC
LINEAR ALGEBRA

Deep Learning

- Deep Learning unterscheidet sich vom Maschinellen Lernen, indem es Maschinen in die Lage versetzt, über die verfügbaren Daten hinaus zu lernen.
- Das beinhaltet die Fähigkeit, Informationen zu analysieren und zu bewerten.
- Um logische Schlüsse zu ziehen, Lösungswege auszuwählen und aus Fehlern zu lernen.
- Je mehr Daten eine Maschine also empfängt, desto grösser ist ihre Lernfähigkeit und desto "intelligenter" kann sie werden.

2. Datenschutz

1. Was ist Datenschutz?



Bearbeiten = jeder Umgang mit Daten

1. Was ist Datenschutz?

Welche Daten werden vom Datenschutz geschützt?

- Es werden **Personendaten** geschützt.
- Personendaten sind Angaben, welche sich auf eine **bestimmte** oder **bestimmbare** natürliche (oder juristische Person) beziehen.

1. Was ist Datenschutz?

Welche Daten werden vom Datenschutz nicht geschützt?

- Nicht geschützt werden Informationen **ohne Personenbezug.**
- Ebenfalls nicht geschützt werden Daten, welche **vollständig anonymisiert** sind, d.h. sie können nicht mehr einer Person zugerechnet werden.

Hochschule Luzern
Informatik

2. Wann ist eine Datenbearbeitung erlaubt?

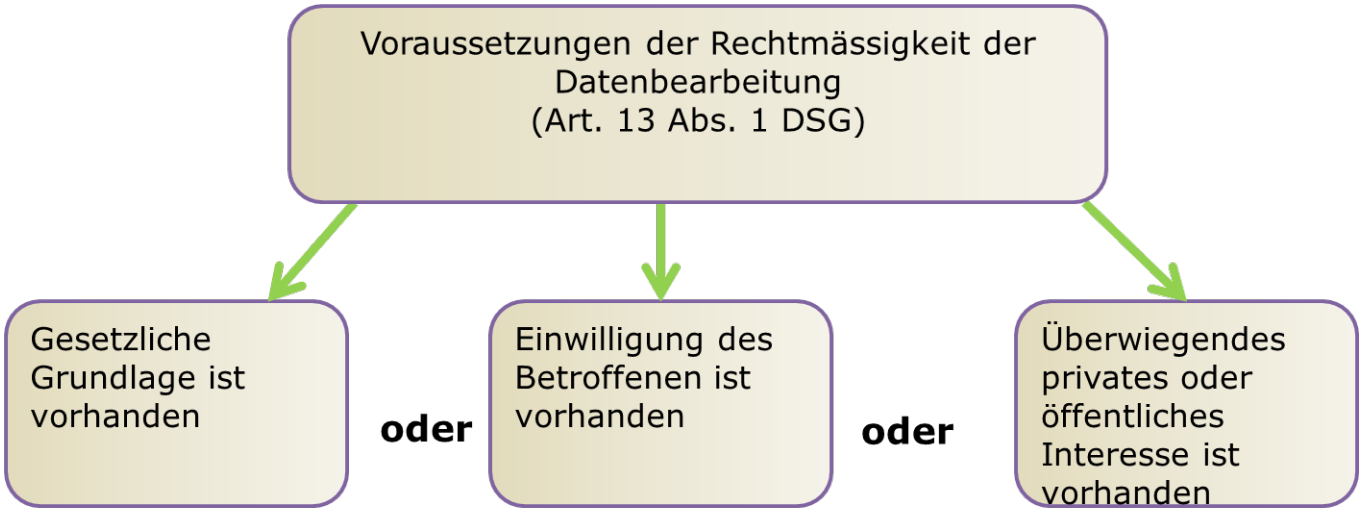
Eine Datenbearbeitung ist legal, wenn sie rechtmässig, verhältnismässig, zweckgebunden und integer ist. Bevor Sie Daten bearbeiten können, müssen Sie folgende vier Fragen mit Ja beantworten können:

- Ist die von mir vorgesehene Bearbeitung der Daten **rechtmässig**?
- Dient die von mir vorgesehene Bearbeitung dem richtigen **Zweck**?
- Ist die von mir vorgesehene Bearbeitung **verhältnismässig**?
- Sind die von mir verwendeten Daten korrekt?

Hochschule Luzern
Informatik

2. Wann ist eine Datenbearbeitung erlaubt?

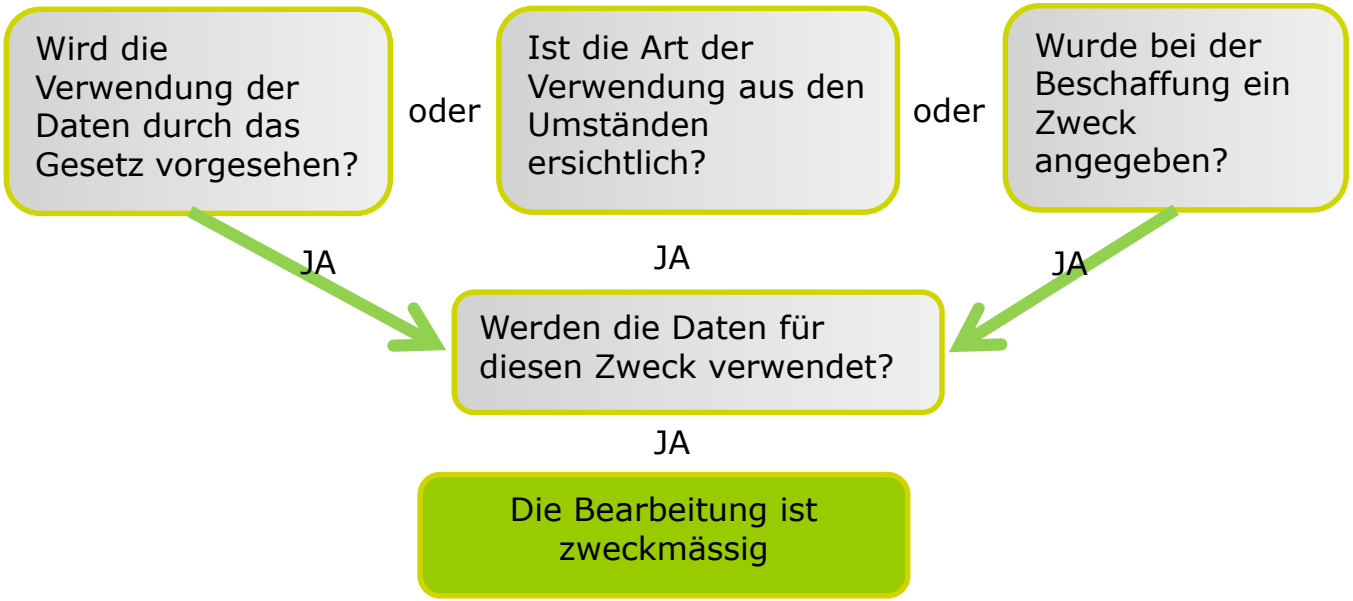
Ist die Bearbeitung rechtmässig?



Hochschule Luzern
Informatik

2. Wann ist eine Datenbearbeitung erlaubt?

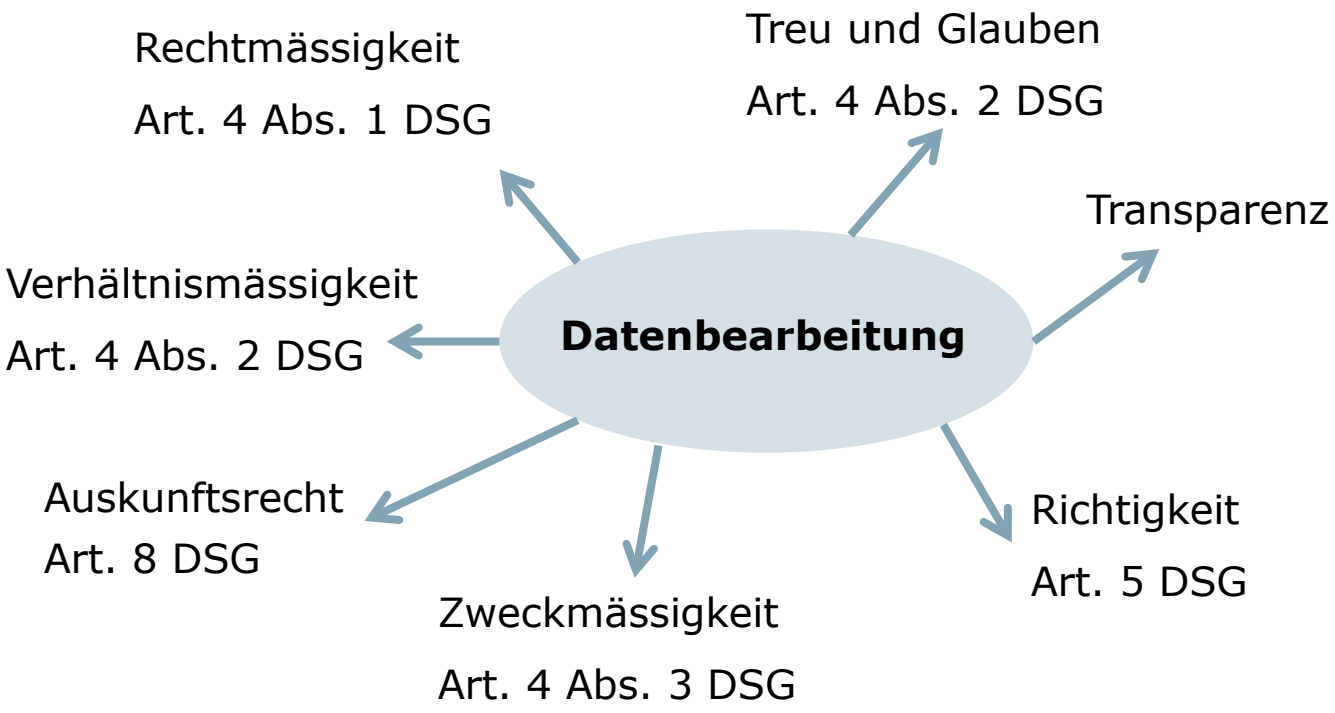
Ist die Bearbeitung zweckmässig?



Bei Zweckänderung muss die Einwilligung der betroffenen Person eingeholt werden.

Hochschule Luzern
Informatik

2. Bearbeitungsprinzipien

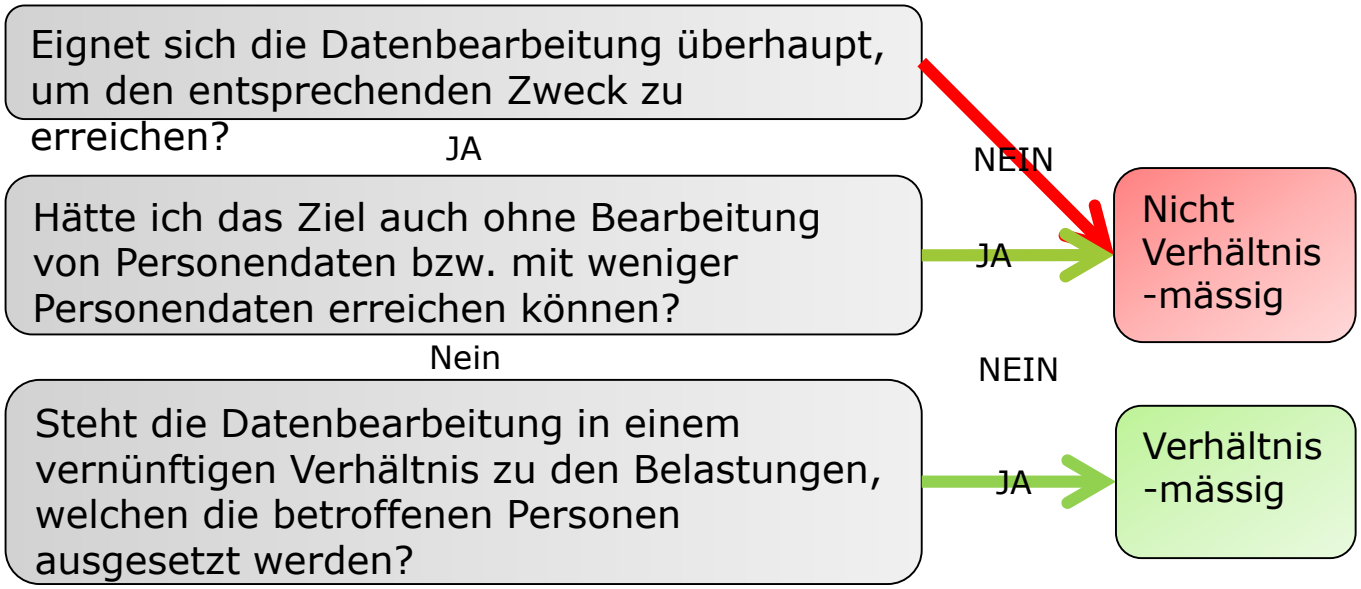


Hochschule Luzern
Informatik

2. Wann ist eine Datenbearbeitung erlaubt?

Ist die Bearbeitung verhältnismässig?

Personendaten dürfen **nur bearbeitet** werden, **sofern** dies **zur Erreichung des Zwecks notwendig** ist. Eine darüber hinaus gehende Bearbeitung ist verboten.



2. Wann ist eine Datenbearbeitung erlaubt?

Wenn Sie alle diese **Fragen** bez. einer Datenbearbeitung **mit Ja** beantworten können, dann ist diese **erlaubt.**

- Ist die von mir vorgesehene Bearbeitung der Daten rechtmässig? 
- Dient die von mir vorgesehene Bearbeitung dem richtigen Zweck? 
- Ist die von mir vorgesehene Bearbeitung verhältnismässig? 
- Sind die von mir verwendeten Daten korrekt? 

3. Spannungsfeld

Fragestellungen

- Darf der Computer die Daten verwenden?
- Sind die Informationen richtig?
- Haben die Resultate weitgehende Konsequenzen für die betroffenen Personen?
- Ist sich die Unternehmensführung der Verantwortung bewusst?
- Sind die Aufsichtsorgane informiert/ involviert?

Art. 5 DSG-Richtigkeit	Künstliche Intelligenz
Art. 5 DSG-Richtigkeit: 1 Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern. Er hat alle angemessenen Massnahmen zu treffen, damit die Daten berichtigt oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind. 2 Jede betroffene Person kann verlangen, dass unrichtige Daten berichtigt werden.	• Beim Beschaffen von Personendaten müssen alle angemessenen Massnahmen ergriffen werden, damit die betroffene Person authentifiziert werden kann und sich die Stichhaltigkeit der erhaltenen Informationen überprüfen lässt • Personendaten, deren Richtigkeit nicht durch angemessene Massnahmen sichergestellt werden kann, dürfen nicht bearbeitet werden oder müssen nach einer bestimmten Zeit zwingend berichtigt oder vernichtet werden. • Der Inhaber der Datensammlung muss die Aktualisierung der beschafften Daten sicherstellen. • Umsetzungsschwierigkeiten für die KI

EU-DSGVO	Künstliche Intelligenz
Art. 22: Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.	• Personen werden zu Objekten von (KI-) Automaten gemacht • automatische Entscheidungsfindung • Profiling Risiko steigt
Art. 33: Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde	• Verletzungen werden nicht erkannt, da die KI implementierte Algorithmen befolgt
Art. 34: Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person	• Verletzungen werden nicht erkannt, da die KI implementierte Algorithmen befolgt

Technologie Folgeabschätzung – Privacy Impact Assessment

- Das Forschungsgebiet der Technikfolgenabschätzung (kurz TA, auch: Technologiefolgenabschätzung oder Technikbewertung) ist ein Teilgebiet der Technikphilosophie und -soziologie.

- Die Technikfolgenabschätzung befasst sich mit der Beobachtung und Analyse von Trends in Wissenschaft und Technik und den damit zusammenhängenden gesellschaftlichen Entwicklungen, insbesondere der Abschätzung der Chancen und Risiken.

- Zudem soll die Technikfolgenabschätzung politische Handlungsempfehlungen oder Richtlinien für die Vermeidung von Risiken und die verbesserte Nutzung der Chancen geben

- Die Stiftung für Technologiefolgen-Abschätzung TA-Swiss (Eigenschreibweise TA-SWISS) ist ein Kompetenzzentrum der Akademien der Wissenschaften Schweiz, dessen Auftrag im Bundesgesetz über die Forschung festgehalten ist.

Privacy by Design & Privacy by Default

Die anfangs 2018 in Kraft tretende Datenschutzgrundverordnung der EU verlangt,
dass bei der Einführung von neuen Dienstleistungen,

Services etc. **technisch und organisatorisch** maximal sichergestellt ist,
dass keine Datenschutzverletzungen vorliegen.

Dies würde bedeuten, dass ohne entsprechende eher generische Einwilligung von **Seiten der betroffenen Personen die Implementierung von Softwareprogrammen der künstlichen Intelligenz häufig illegal wäre**. Dies ist nämlich der Fall, sobald ein Programm Aktivitäten entwickelt, welche nicht genau im Vornherein durch eine gesetzliche Grundlage abgedeckt sind.

Künstliche Intelligenz:

- **implementierte Algorithmen und Methodologie**
- **automatisierte Entscheidungsfindung**
- **Ausgrenzung oder gar Diskriminierung bestimmter Personen(kreise)**

Fazit

- Programme und Roboter weisen immer mehr menschliche Verhaltensmuster auf und scheinen der menschlichen Intelligenz teilweise sogar überlegen zu sein.
- Selbstlernende Computerprogramme gewinnen für zukünftige Entwicklungen zur Digitalisierung der Gesellschaft immer mehr an Bedeutung.
- Für die (zulässige) Bearbeitung von Personendaten bedarf es der Einhaltung verschiedener Regeln. So werden eine gesetzliche Grundlage oder eine Einwilligung der betroffenen Personen sowie die Verhältnismässigkeit der Datenbearbeitung vorausgesetzt.
- Welche Schlüsse Systeme künstlicher Intelligenz ziehen, lässt sich schwer vorhersehen. Eine Einwilligung einzuholen ist schwierig, weil die betroffene Person für eine wirksame Einwilligung wissen muss, in was sie einwilligt.
- Es stellt sich die Frage, ob es möglich ist, die Einwilligung für die Methodologie und die Anwendung des Algorithmus einzuholen verbunden mit einem jederzeitigen Informations- und Auskunftsrecht und der Möglichkeit auf Löschung dieser Daten.
- Die Datenschutzverordnung der EU sind Aktivitäten von Softwareprogrammen, welche im Vornherein nicht genau durch eine gesetzliche Grundlagen abgedeckt sind, illegal.

Fragen?

Danke

Publikationen:

- Handbücher für die Anwaltspraxis – Haftung und Versicherung, **Kapitel „IT-Fehler“ von Ursula Sury**

  Helbling & Lichtenhahn Verlag, 2015

- Prinzipen des Vertragsrechts, **Kapitel „IT-Outsourcing Verträge“ von Ursula Sury**

  Schulthess-Verlag, 2015

- Immaterialgüterrecht in kommentierten Leitentscheiden, **Kapitel „BGE 125 III 263: Softwarelizenz: Wie weit reichen die Nutzungsrechte der Lizenznehmerin?“ von Ursula Sury**

  Schulthess-Verlag, 2015

Danke

Publikationen:

- **Kurzeinführung ins Arbeitsrecht - von der Vertragsanbahnung bis zur Kündigung**

  Sprenger/Sury/Seger, Stämpfli Verlag, 2013

- **Informatikrecht**

  Sury Ursula, Stämpfli Verlag, 2013

- Beitrag **„Recht im Offshoring“,**

  In: IT-Offshoring - Potenziale, Risiken, Erfahrungsberichte

  Sury Ursula, Orell Füssli Verlag Zürich, 2006.

Danke

Beiträge Ursula Sury in: IT-business

Gelöscht? Vergessen? Oder für immer im Netz?	Ausgabe 2/2019
Datenschutzrevisionen und Auswirkungen auf die Softwareentwicklung	Ausgabe 1/2017

Beiträge Ursula Sury in: Informatik Spektrum
(Springer-Verlag)

Distributed Ledger und Governance	Heft 5/2019
Auftragsdatenverarbeitung	Heft 4/2019
E-Contracting	Heft 2/2019
Cyberverantwortung	Heft 1/2019
Deep Learning und Rechtsrisiken	Heft 6/2018
Token und Recht	Heft 5/2018
Guter Glaube und Vertrauen bei Blockchain	Heft 4/2018
Datenschutz CH und EU: Was wird wirklich neu?	Heft 3/2018
Blockchain und Datenschutz	Heft 2/2018
DAO und Rechtsaspekte	Heft 1/2018
Smart Contracts	Heft 4/2017

Danke

DIE
ADVOKATUR
SURY

www.dieadvokatur.ch
info@dieadvokatur.ch

Lucerne University of
Applied Sciences and Arts
HOCHSCHULE
LUZERN

www.hslu.ch

RA Ursula Sury
Die Advokatur Sury AG
Alpenquai 4
6005 Luzern