

# Vorlesung Digitale Nachhaltigkeit

## Termin 5: Datenschutz und Privatsphäre

19. Oktober 2022

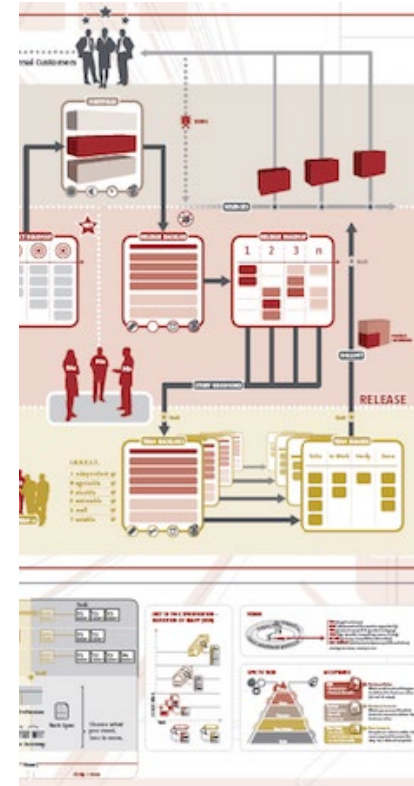
**PD Dr. Matthias Stürmer**

Forschungsstelle Digitale Nachhaltigkeit  
Institut für Informatik  
Universität Bern



# Termine

1. **21. September 2022:** Einführung und Überblick
2. **28. September 2022:** Ökologische Nachhaltigkeit und Digitalisierung
3. **5. Oktober 2022:** Soziale Nachhaltigkeit und Digitalisierung
4. **12. Oktober 2022:** Konzept der digitalen Nachhaltigkeit
5. **19. Oktober 2022:** Datenschutz und Privatsphäre
6. **26. Oktober 2022:** Ethische Fragestellungen bei KI
7. **2. November 2022:** Urheberrecht und Lizenzen
8. **9. November 2022:** Open Source Software Development
9. **16. November 2022:** Open Source Communities
10. **23. November 2022:** Geschäftsmodelle in der IT-Branche
11. **30. November 2022:** Digital nachhaltige Unternehmens-IT
12. **7. Dezember 2022:** Digitale Transformation in der Schweiz
13. **14. Dezember 2022:** Mündliche Präsentationen Teil 1
14. **21. Dezember 2022:** Mündliche Präsentationen Teil 2



# Heutiges Gastreferat

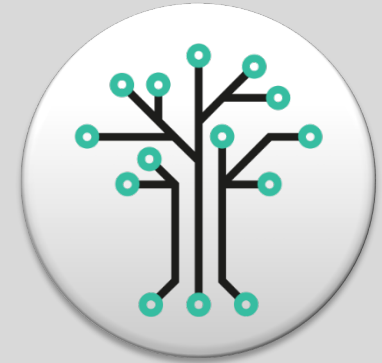
## **Dr. iur. Benjamin Domenig:**

- Co-Gründer und Partner  
Domenig & Partner Rechtsanwälte AG
- Dr. iur. Universität St.Gallen (HSG)
- Studium Universität St.Gallen (HSG),  
Universität Bern, Universität Lausanne  
und University of Texas in Austin
- Anwaltspatent im Kanton Bern
- Vorstand Verein Digital Impact Network



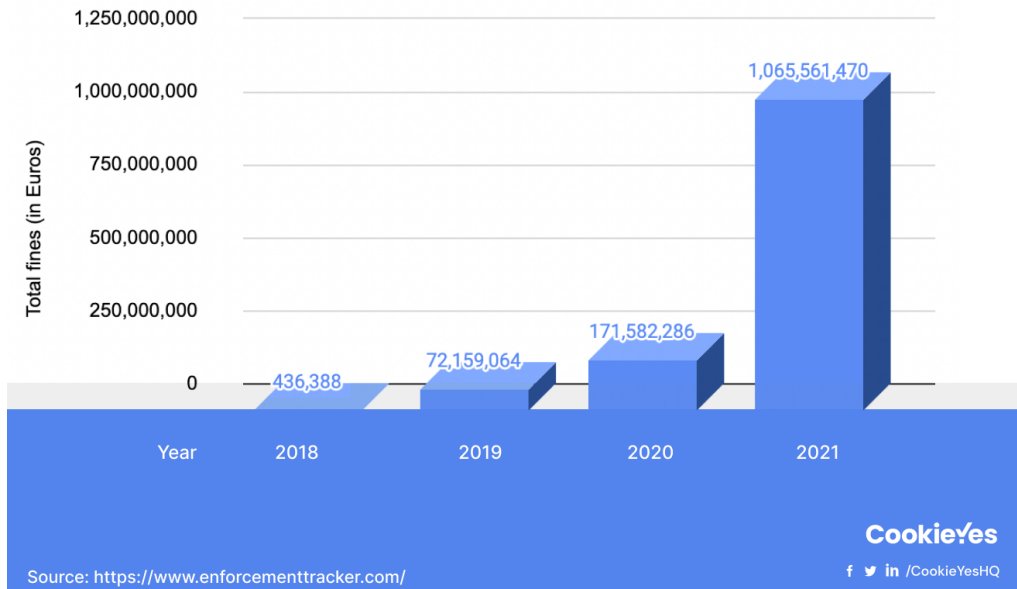
# Agenda

1. **Einführung zum Datenschutz**
  2. Basics der Datenschutzgrundverordnung
  3. Daten-Anonymisierung durch k-anonymity
- Informationen zur mündlichen Präsentation und schriftlichen Arbeit



# Relevanz neues EU-Datenschutzgesetz

## Total GDPR Fines (in Euros) (2018-2021)



## DSGVO-Bussen erreichen 2021 über 1 Milliarde Euro

Gegen die EU-Datenschutz-Grundverordnung wurde im Jahr 2021 mehrfach verstoßen. Es mussten DSGVO-Bussen in der Höhe von insgesamt über 1 Milliarde Euro ausgesprochen werden. Das ist ein massiver Anstieg gegenüber dem Jahr 2020.

Thomas Berner - 07. Januar 2022



# Bussgelder-Rechner und effektive Bussen

## Bußgeldrechner: DSGVO-Verstöße

**DSGVO Bußgeldrechner 2022**

Vorjahresumsatz

Art des Verstoßes

Schweregrad

Lizenz von Smart-Rechner  
Datenschutzutzerklärung

**Berechnen**

**Berechnung**

Bußgeld Minimum 19 444 €

Bußgeld Mittelwert 29 166 €

Bußgeld Maximum 38 888 €

Herleitung der Bußgeldberechnung

Leistungsbeschreibung

**Herleitung der Bußgeldberechnung**

Gemäß des Bußgeldkonzepts des DSK erfolgen folgende Berechnungsschritte:

1. Kategorisierung der Unternehmensgröße

Anhand des angegebenen Umsatzes in Höhe von bis zu 5,0 Mio. Euro ist das

## Geldbußen für DSGVO-Verstöße

und für Verletzungen anderer Datenschutzgesetze

Datum	Bußgeld	Empfänger	Land	Vergehen
24.07.2019	4.536.999.350 €	Facebook, Inc.	US	Verstoß gegen frühere FTC-Datenschutzanordnungen und FTC-Gesetz <a href="#">»Details</a>
21.07.2022	1.165.011.903 €	DiDi	CN	Verstöße gegen Gesetze zur Netzwerksicherheit, Datensicherheit und zum Schutz persönlicher Informationen. <a href="#">»Details</a>
30.07.2021	746.000.000 €	Amazon Europe Core S.à r.l	LU	Verstöße im Zusammenhang mit der Anzeige von Werbung und der Weitergabe von Daten an Dritte. <a href="#">»Details</a>
22.07.2019	508.130.081 €	Equifax Inc.	US	Unzureichende Schutzmaßnahmen ermöglichten Diebstahl von Bonitätsdaten von 147 Mio. Betroffenen. <a href="#">»Details</a>
05.09.2022	405.000.000 €	Instagram	IE	Rekordbußgeld für Instagram nach Bruch von Datenschutzrechten Minderjähriger. <a href="#">»Details</a>
02.09.2021	225.000.000 €	WhatsApp Ireland Ltd.	IE	Verletzung der Informationspflichten, insbesondere bzgl. Datenübermittlung an andere Facebook-Unternehmen. <a href="#">»Details</a>
25.05.2022	140.765.766 €	TWITTER, INC.	US	Unberechtigte Verwendung der E-Mail-Adressen und Telefonnummern von Nutzern zur personalisierten Werbung. <a href="#">»Details</a>
06.01.2022	90.000.000 €	GOOGLE LLC	FR	Keine Möglichkeit, Cookies auf www.google.fr und www.youtube.com ebenso einfach abzulehnen wie sie anzunehmen. <a href="#">»Details</a>

# Wozu braucht es Datenschutz überhaupt?

- **«Personendaten sind ein wertvolles Gut.»**
- **Materielle Sichtweise:**
  - Wirtschaftliches Potential für Unternehmen
  - Persönlichkeitsprofile von Einzelpersonen → Zielgruppen bilden
  - Ohne Einschränkungen wäre Missbrauchspotential hoch
- **Ideelle Sichtweise:**
  - Informationelle Selbstbestimmung → Welche Daten will ich freigeben?
  - Staat will auch Daten → Was ist legitim, was zu viel Überwachung?
- **Verhältnismässigkeit** → nur so viele persönliche Daten wie nötig und so wenig persönliche Daten wie möglich
- **Auskunftsrecht** → Rechenschaft über die Datensammlung




**Adrian Lobsiger**

Eidgenössischer  
Datenschutz- und  
Öffentlichkeitsbeauftragter  
(EDÖB)



# Neues Schweizer Datenschutzgesetz




Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD  
**Bundesamt für Justiz BJ**  
Direktionsbereich Öffentliches Recht  
Fachbereich Rechtsetzungsprojekte I

Bundesverwaltung > Departement: EJPD > Bundesamt für Justiz BJ

Startseite



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

**Der Bundesrat**

Aktuell	Staat & Bürger	Gesellschaft	Wirtschaft	Sicherheit	Publikationen & Service	Das BJ
---------	----------------	--------------	------------	------------	-------------------------	--------

Startseite > Aktuell > Medienmitteilungen > Neues Datenschutzrecht ab 1. September 2023

< Startseite

**Aktuell**

Medienmitteilungen

Informationen

Reden & Interviews

Veranstaltungen

Coronavirus und Justiz

## Neues Datenschutzrecht ab 1. September 2023

Bern, 31.08.2022 - Das totalrevidierte Datenschutzgesetz (DSG) und die Ausführungsbestimmungen in der neuen Datenschutzverordnung (DSV) und der neuen Verordnung über Datenschutzzertifizierungen (VDSZ) treten am 1. September 2023 in Kraft. Das hat der Bundesrat an seiner Sitzung vom 31. August 2022 entschieden. Damit erhält die Wirtschaft genügend Zeit, die notwendigen Vorkehrungen für die Umsetzung des neuen Datenschutzrechts zu treffen.

Das totalrevidierte DSG und die entsprechenden Bestimmungen in den Verordnungen sorgen künftig für einen besseren Schutz der persönlichen Daten. Insbesondere werden der Datenschutz den technologischen Entwicklungen angepasst, die Selbstbestimmung über die persönlichen Daten gestärkt sowie die Transparenz bei der Beschaffung von Personendaten erhöht.

Um den Ergebnissen der Vernehmlassung zu den Ausführungsbestimmungen Rechnung zu tragen, hat der Bundesrat den Entwurf der DSV in mehreren Punkten angepasst. So hat er das Kapitel zu den Pflichten der Verantwortlichen eingehend überarbeitet und insbesondere die Privaten von gewissen Informationspflichten bei der Bekanntgabe von Personendaten befreit. Auch die Modalitäten zum Auskunftrecht wurden vereinfacht und



# Besonders schützenswerte Personendaten

→ Wichtiger Begriff im Schweizer Datenschutzgesetz (**neues Gesetz**)

## Besonders schützenswerte Personendaten:

1. Daten über **religiöse, weltanschauliche, politische oder gewerkschaftliche** Ansichten oder Tätigkeiten,
2. Daten über die **Gesundheit**, die **Intimsphäre** oder die **Zugehörigkeit** zu einer **Rasse** oder **Ethnie**,
3. **genetische Daten**,
4. **biometrische Daten**, die eine natürliche Person eindeutig identifizieren,
5. Daten über **verwaltungs- und strafrechtliche** Verfolgungen oder Sanktionen,
6. Daten über Massnahmen der **sozialen Hilfe**

# Unterschied Datenschutz & Datensicherheit

## Datenschutz:

- Schutz von personenbezogenen Daten
- Recht der informationellen Selbstbestimmung
- Datenschutzgesetz zur Erhebung, Verarbeitung und Nutzung von personenbezogene Daten durch Firmen und staatliche Stellen

## Datensicherheit:

- Genereller Schutz von Daten, egal ob mit oder ohne Personenbezug
- Schutz der Daten vor Hackerangriffe, Verlust, Zerstörung etc.
- Technische Massnahmen

# Data Security vs. Data Privacy

## Data Protection

### Security

Encryption

Network  
Security

Access  
Control

Activity  
Monitoring

Breach  
Response

DLP/CASB

How those policies got enforced

### Privacy

Discovery &  
Classification

DSARs

Alerting

Regulations

Contracts

Policies

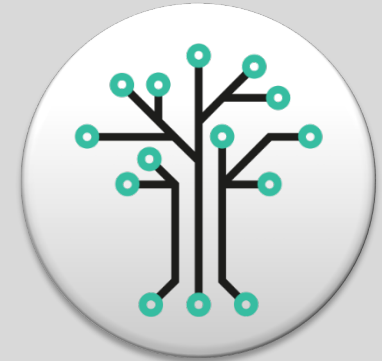
What data is important and why

Protected  
Usable  
Data

# Agenda

1. Einführung zum Datenschutz
2. **Basics der Datenschutzgrundverordnung**
3. Daten-Anonymisierung durch k-anonymity

→ Informationen zur mündlichen Präsentation  
und schriftlichen Arbeit



# Begriffe und historische Entwicklung

## Begrifflichkeiten:

- Auf Deutsch «DSGVO»: **Datenschutzgrundverordnung**
- Auf Englisch “GDPR”: **General Data Protection Regulation**

## Historische Entwicklung:

- 2012 Vorschlag der EU-Kommission für mehr Privatsphäre im Internet
- 2014 Zustimmung durch EU-Parlament
- 27. April 2016 Beginn der DSGVO mit Übergangsfrist von 2 Jahren
- 25. Mai 2018 Inkrafttreten der DSGVO

# 7 Prinzipien der DSGVO

1. Rechtmässigkeit
2. Zweckbindung
3. Datenminimierung
4. Richtigkeit
5. Speicherbegrenzung
6. Integrität und Vertraulichkeit
7. Rechenschaftspflicht



# 1. Rechtmässigkeit

Personenbezogene Daten müssen ...

- auf **rechtmässige Weise** verarbeitet werden
- nach **Treu und Glauben** und
- in einer für die betroffene Person **nachvollziehbaren Weise**



**Be Transparent  
With Data**

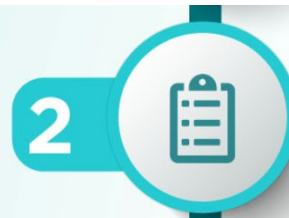
Implied consent is  
a big no-no under  
the GDPR.



## 2. Zweckbindung

Personenbezogene Daten müssen ...

- für **festgelegte, eindeutige und legitime Zwecke** erhoben werden
- und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise **weiterverarbeitet werden**



**Limit Data to  
What You Need**

No scooping up  
data just because  
you can.

## 3. Datenminimierung

Personenbezogene Daten müssen ...

- dem **Zweck angemessen** und erheblich
- sowie auf das für die **Zwecke der Verarbeitung** notwendige Mass beschränkt sein



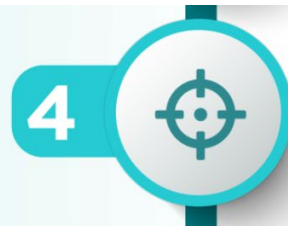
**Limiting  
Kept Data**

Do we need all this  
data? If the answer  
is no, delete it.

## 4. Richtigkeit

Personenbezogene Daten müssen ...

- **sachlich richtig**
- und erforderlichenfalls auf dem **neuesten Stand** sein.
- Falsche Daten unverzüglich **löschen oder berichtigen**



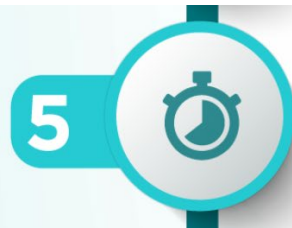
**Data Must  
be Accurate**

Make sure that data  
is accurate and  
up-to-date.

## 5. Speicherbegrenzung

Personenbezogene Daten müssen ...

- in einer Form **gespeichert** werden,
- die die **Identifizierung** der betroffenen Personen nur so lange ermöglicht, wie es für die **Zwecke**, für die sie verarbeitet werden, erforderlich ist.
- Ausnahmen: **Historische Zwecke** oder für **Statistiken**



**Limit Storage of  
Personal Data**

**Don't keep it longer  
than you need it.**

## 6. Integrität und Vertraulichkeit

Personenbezogene Daten müssen ...

- in einer Weise verarbeitet werden, die eine angemessene **Sicherheit** der personenbezogenen Daten gewährleistet,
- einschliesslich Schutz vor unbefugter oder unrechtmässiger **Verarbeitung** und vor unbeabsichtigtem **Verlust**,
- unbeabsichtigter **Zerstörung** oder unbeabsichtigter Schädigung
- durch geeignete technische und organisatorische **Massnahmen**



## 7. Rechenschaftspflicht

- Der/die Verantwortliche ist für die **Einhaltung der DSGVO** verantwortlich und muss dessen Einhaltung nachweisen können
- Unternehmen sind gegenüber den Aufsichtsbehörden in der **Nachweispflicht**.



# Wichtige Bestimmungen der DSGVO



## Geltungsbereich

Die DSGVO gilt unabhängig von ihrem Standort für alle Unternehmen, die personenbezogene Daten von EU-Bürgern verarbeiten.



## Geldbußen

Geldbußen können bis zur Höhe von zwei Millionen Euro verhängt werden oder im Fall von Unternehmen bis zu vier Prozent des gesamten weltweit erzielten Umsatzes des vorangegangenen Geschäftsjahres, je nachdem, welcher Betrag höher ist.



## Einwilligung

Die Einwilligung muss freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich erteilt werden. Sie muss so einfach zurückgezogen werden können, wie sie erteilt wurde.



# Wichtige Bestimmungen der DSGVO



## Meldepflicht

Eine Datenschutzverletzung muss unverzüglich und möglichst innerhalb von 72 Stunden, nachdem sie dem Unternehmen bekannt wurde, der Aufsichtsbehörde gemeldet werden. Die betroffenen Personen müssen ebenfalls informiert werden.



## Auskunftsrecht

Die EU-Bürger haben das Recht, vom Datenverantwortlichen zu erfahren, ob personenbezogene Daten, die sie betreffen, verarbeitet werden, wo sie sie verarbeitet werden und zu welchem Zweck.



## Recht auf Löschung

Die EU-Bürger können vom Datenverantwortlichen unter bestimmten Voraussetzungen verlangen, dass ihre ihm zur Verfügung gestellten personenbezogenen Daten unverzüglich gelöscht werden.

# Wichtige Bestimmungen der DSGVO



## Datenübertragbarkeit

Die EU-Bürger können die personenbezogenen Daten, die sie einem Unternehmen bereitgestellt haben, anfordern und sie einem anderen Unternehmen übertragen. Der Datenverantwortliche muss die Daten in einem strukturierten, gängigen und maschinenlesbaren Format übermitteln.



## Nur eine Anlaufstelle

Unternehmen, die in mehreren EU-Staaten aktiv sind, ermöglicht die DSGVO die Zusammenarbeit mit nur einer, nämlich ihrer lokalen Aufsichtsbehörde. Die einheitliche Anwendung der DSGVO wird durch einheitliche Abläufe und die EU-weite Zusammenarbeit der Behörden sichergestellt.



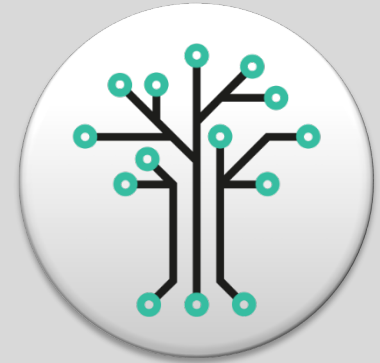
## Datenschutzbeauftragter

Unter bestimmten Bedingungen müssen Datenverantwortliche und Auftragsverarbeiter einen Datenschutzbeauftragten ernennen (im Rahmen ihrer Rechenschaftspflicht). Er steuert und überwacht im Unternehmen alle Aktivitäten im Zusammenhang mit dem Datenschutz.

# Agenda

1. Einführung zum Datenschutz
2. Basics der Datenschutzgrundverordnung
3. **Daten-Anonymisierung durch k-anonymity**

→ Informationen zur mündlichen Präsentation  
und schriftlichen Arbeit



# Latanya Sweeney

- 2001 erste African-American Frau, die **PhD am MIT** erhielt
- Gründerin und Direktorin des Data Privacy Lab der **Carnegie Mellon Universität**
- Heute Professorin der Practice of Government and Technology an der **Harvard-Universität**
- Über 100 wissenschaftliche Publikationen



# k-Anonymity

- **Trade-off** zwischen Offenheit und Datenschutz
- k-anonymity Verfahren von **Latanya Sweeney** in 2001
- «k» ist die kleinste **Zahl von Personen mit gleichen Werten**
- Beispiel: **Notentabelle**

Student	Number	Gender	Birth	Location	Grade
Michael Müller	15-456-984	male	26.08.1995	Bern	5.0
Sabrina Meier	09-154-367	female	04.04.1994	Thun	6.0
Raphael Ritter	11-059-128	male	16.12.1996	Bern	4.0
Marc Ospelt	13-747-175	male	22.12.1993	Köniz	6.0
Flavia Polli	19-130-715	female	20.04.1996	Zürich	4.5
Isabelle Kunz	13-567-698	female	23.12.1981	Bern	5.0
Dario Schmid	17-102-534	male	06.05.1996	Bern	5.5
Lena Lutz	07-054-331	female	03.08.1990	Thun	5.0
Clemens Steiner	09-115-056	male	27.07.1996	Belp	4.5
Christian Singer	13-117-718	male	22.07.1996	Lyss	4.0
Tanja Haudenschild	95-104-675	female	17.02.1997	Laufen	3.5
Stefanie Stalder	15-116-437	female	01.12.1998	Thun	4.5
Sara Tschannen	11-072-584	female	14.09.1983	Bern	6.0
Marco Salzmann	16-059-701	male	19.05.1998	Basel	5.0
Claudio Hofer	10-055-739	male	23.03.1997	Thun	4.5

# k-Anonymity

- **Identifiers entfernen:** Name und Matrikelnummer
- **Quasi-Identifiers entfernen:** Tag und Monat des Geburtsdatum
- Darf diese Tabelle so **publiziert** werden?

Student	Number	Gender	Birth	Location	Grade
*	*	male	1995	Bern	5.0
*	*	female	1994	Thun	6.0
*	*	male	1996	Bern	4.0
*	*	male	1993	Köniz	6.0
*	*	female	1996	Zürich	4.5
*	*	female	1981	Bern	5.0
*	*	male	1996	Bern	5.5
*	*	female	1990	Thun	5.0
*	*	male	1996	Belp	4.5
*	*	male	1996	Lyss	4.0
*	*	female	1997	Laufen	3.5
*	*	female	1998	Thun	4.5
*	*	female	1983	Bern	6.0
*	*	male	1998	Basel	5.0
*	*	male	1997	Thun	4.5

# k-Anonymity

- Nein, weil die meisten Datensätze **eindeutig** sind (rote Linien)
- Personen lassen sich **re-identifizieren**
- Bspw. wenn **Open Data** verwendet wird
- Bspw. in einer **kleinen Gemeinde**

Student	Number	Gender	Birth	Location	Grade
*	*	male	1995	Bern	5.0
*	*	female	1994	Thun	6.0
*	*	male	1996	Bern	4.0
*	*	male	1993	Köniz	6.0
*	*	female	1996	Zürich	4.5
*	*	female	1981	Bern	5.0
*	*	male	1996	Bern	5.5
*	*	female	1990	Thun	5.0
*	*	male	1996	Belp	4.5
*	*	male	1996	Lyss	4.0
*	*	female	1997	Laufen	3.5
*	*	female	1998	Thun	4.5
*	*	female	1983	Bern	6.0
*	*	male	1998	Basel	5.0
*	*	male	1997	Thun	4.5



# k-Anonymity

- Darum müssen weitere Informationen entfernt werden, bspw. das **exakte Geburtsjahr**
- Jedoch hat es immer noch **einige eindeutige Datensätze** (rote Linien)

Student	Number	Gender	Birth	Location	Grade
*	*	male	199*	Bern	5.0
*	*	female	199*	Thun	6.0
*	*	male	199*	Bern	4.0
*	*	male	199*	Köniz	6.0
*	*	female	199*	Zürich	4.5
*	*	female	198*	Bern	5.0
*	*	male	199*	Bern	5.5
*	*	female	199*	Thun	5.0
*	*	male	199*	Belp	4.5
*	*	male	199*	Lyss	4.0
*	*	female	199*	Laufen	3.5
*	*	female	199*	Thun	4.5
*	*	female	198*	Bern	6.0
*	*	male	199*	Basel	5.0
*	*	male	199*	Thun	4.5

# k-Anonymity

- Darum auch **Wohnort** anonymisieren
- Jetzt ist **2-anonymity** (k=2) weil minimal zwei Datensätze identisch sind (ausser sensibler Wert)
- **Äquivalenzklasse:** Gruppe von Personen mit gleichen Attributen

Student	Number	Gender	Birth	Location	Grade
*	*	male	199*	*	5.0
*	*	female	199*	*	6.0
*	*	male	199*	*	4.0
*	*	male	199*	*	6.0
*	*	female	199*	*	4.5
*	*	female	198*	*	5.0
*	*	male	199*	*	5.5
*	*	female	199*	*	5.0
*	*	male	199*	*	4.5
*	*	male	199*	*	4.0
*	*	female	199*	*	3.5
*	*	female	199*	*	4.5
*	*	female	198*	*	6.0
*	*	male	199*	*	5.0
*	*	male	199*	*	4.5

# Problem: Homogenitätsattacke

- Sensible Daten einer Äquivalenzklasse können **identisch** sein
- Lösung: sensible Daten müssen **variieren**

Student	Number	Gender	Birth	Location	Grade
*	*	male	199*	*	5.0
*	*	female	199*	*	6.0
*	*	male	199*	*	4.0
*	*	male	199*	*	6.0
*	*	female	199*	*	4.5
*	*	female	198*	*	5.0
*	*	male	199*	*	5.5
*	*	female	199*	*	5.0
*	*	male	199*	*	4.5
*	*	male	199*	*	4.0
*	*	female	199*	*	3.5
*	*	female	199*	*	4.5
*	*	female	198*	*	5.0
*	*	male	199*	*	5.0
*	*	male	199*	*	4.5

# Problem: Background Knowledge Attack

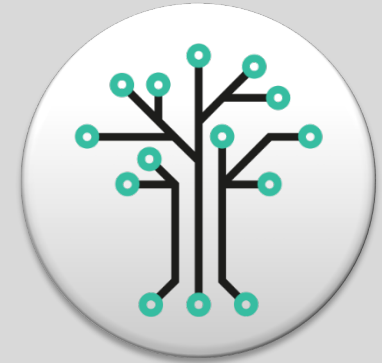
- **Zusätzliche Information** kann sensible Daten einer Person enthüllen
- Bspw. kennt jemand **beide Frauen** mit **Jahrgang 198\***
- Zusätzlich ist von einer Studentin bekannt, **dass sie eine 6 hat...**

Student	Number	Gender	Birth	Location	Grade
*	*	male	199*	*	5.0
*	*	female	199*	*	6.0
*	*	male	199*	*	4.0
*	*	male	199*	*	6.0
*	*	female	199*	*	4.5
*	*	female	198*	*	3.0
*	*	male	199*	*	5.5
*	*	female	199*	*	5.0
*	*	male	199*	*	4.5
*	*	male	199*	*	4.0
*	*	female	199*	*	3.5
*	*	female	199*	*	4.5
*	*	female	198*	*	6.0
*	*	male	199*	*	5.0
*	*	male	199*	*	4.5

# Agenda

1. Einführung zum Datenschutz
2. Basics der Datenschutzgrundverordnung
3. Daten-Anonymisierung durch k-anonymity

**→ Informationen zur mündlichen Präsentation  
und schriftlichen Arbeit**



# Mündliche Präsentation

- **Präsentation** eines Vertiefungsthemas aus der Vorlesung an den zwei letzten Terminen, **Mittwoch, 14. und 21. Dezember 2022 von 9:15h bis 12:00h**
- Präsentation wird **benotet** (Gruppennote), zählt **50%** zur Gesamtnote
- **Ziele der mündlichen Präsentation:**
  1. Vertiefte inhaltliche Auseinandersetzung mit einem Fokus-Thema
  2. Präsentations-Skills üben → alle Gruppenmitglieder sollen vortragen
  3. Zusammenarbeit im Team, Diskussion zu gesellschaftlichem Thema
- Aktuell sind **28 Gruppen** auf ILIAS eingetragen
- Wenn noch jemand **keine Gruppe** hat, umgehend bei Lena und Joel melden

# Form und Inhalt mündliche Präsentation

**Form:** Kurzvortrag vor Ort, ca. 8min mit PowerPoint Slides (Vorlage folgt)

**Themenwahl:** Thema von einer der 11 Vorlesungstermine wählen, dann Vertiefungsrichtung festlegen, bspw. zum heutigen Thema «Datenschutz und Privatsphäre» das *EU-US Privacy Shield* und das *Schrems II Urteil* vorstellen

## **Aufbau der Präsentation:**

- 1. Wissenschaftlicher Teil:** relevante Publikationen und Berichte recherchieren und kurz vorstellen
- 2. Praktischer Teil:** konkrete Beispiele und Fälle aus der Praxis aufzeigen
- 3. Persönliches Fazit:** eigene Schlussfolgerungen, neue Erkenntnisse etc.



## Zeitlicher Ablauf mündliche Präsentation

- Bis spätestens **23. November 2022** Thema und Titel in der Gruppenbeschreibung angeben, bspw: «Datenschutz und Privatsphäre: EU-US Privacy Shield»
  - Bis spätestens **7. Dezember 2022** Folien in ILIAS hochladen
  - Am **Mittwoch, 14. oder 21. Dezember 2022** zwischen 9:15h und 12:00h in Bern vor Ort den Kurzvortrag halten
- Bei Fragen, Anliegen etc. frühzeitig bei Lena und Joel melden!

# Schriftliche Arbeit

- **4 Fragen zu 3 der insgesamt 11 Vorlesungs-Themen beantworten:**
  1. Welches sind die Vorteile/Chancen/Potential dieses Themas für die Gesellschaft?
  2. Welches sind die Nachteile/Gefahren/Probleme/Herausforderungen für die Gesellschaft?
  3. Was für neue Entwicklungen gibt es in diesem Thema?
  4. Was ist Ihre Meinung zu diesem Thema?
- **Je ca. ½ Seite Fliesstext pro Frage** (1500 – 1800 Zeichen mit Leerzeichen),  
**insgesamt ca. 6 Seiten** (18'000 – 22'000 Zeichen mit Leerzeichen)
- **Abgabe bis 15. Januar 2023** als PDF in ILIAS hochladen
- **Beurteilungskriterien** der schriftlichen Arbeit:
  1. Vollständigkeit und Nachvollziehbarkeit der Vorteile etc.
  2. Vollständigkeit und Nachvollziehbarkeit der Nachteile etc.
  3. Neuartigkeit und Qualität der gefundenen Informationsquellen
  4. Überzeugende Begründung der eigenen Meinung
  5. Gesamtqualität der Antworten (Struktur, Grammatik, Orthografie, Formatierung etc.)

# Inhaltliche Hinweise zur schriftlichen Arbeit

- Keine Seminararbeit zu neuem Thema, sondern **Verarbeitung** (gute Zusammenfassung) und **Reflexion** von **drei Themen** aus der Vorlesung
- **Gastreferat** (falls vorhanden) ist integraler Teil des Termins
- Mit «Thema» ist **‘Über-Thema’ des Vorlesungstermins** gemeint, nicht nur ein ‘Detail-Thema’ innerhalb des Termins, bspw.
  - Ökologische Aspekte der Digitalisierung, nicht nur Rebound-Effekt
  - Soziale Aspekte der Digitalisierung, nicht nur Gesichtserkennung
  - Datenschutz und Privatsphäre, nicht nur k-Anonymity
- Immer **Vor- und Nachteile** des Themas anhand erwähnter Beispiele behandeln, bspw.
  - Potential vs. Probleme der Digitalisierung aus ökologischer Sicht
  - Potential der Datennutzung vs. Gefahr der Datennutzung (darum braucht es Datenschutz)
- Immer **Fokus auf die Digitalisierung**, also bspw. nicht Nachhaltigkeit allgemein

# Weitere Vorgaben zur schriftlichen Arbeit

- **Ziele der schriftlichen Arbeit sind:**
  - a) Zusammenfassung der Vorteile und Nachteile des Themas aus dem Unterricht (keine neuen Quellen notwendig)
  - b) Eigene Recherche zum Thema, was im Unterricht gefehlt hat, was grad aktuell in den Medien diskutiert wird etc. (Einbezug neuer Quellen)
  - c) Persönliche Meinung bilden und gut vermitteln (Begründung)
- **Deutsch oder Englisch**
- **Wissenschaftliche, neutrale, objektive, nüchterne Sprache**, nicht polemisch oder pathetisch, ausser bei Teil 4 „Persönliche Meinung“
- **LibreOffice- oder Word-Vorlage** verwenden (folgt in ILIAS)

# Zur Struktur der schriftlichen Arbeit

**Zu allen drei Themen der drei Vorlesungstermine die folgenden Punkte beantworten:**

1. **Vorteile:** Zusammenfassung der Chancen, Potentiale etc. von diesem Thema (aus dem Unterricht) → bspw. neue Möglichkeiten der Datenverwendung, Nutzen für die Wirtschaft
2. **Nachteile:** Zusammenfassung der Probleme, Herausforderungen, aufzeigen von Lösungsansätzen (falls vorhanden) → bspw. Missbrauch der Datenverwendung, darum Datenschutz
3. **Weitere Quellen, neue Aspekte:** was hat gefehlt, was kam zu kurz, was gibt's Aktuelles → neue Perspektiven auf das Thema aufzeigen durch zusätzliche Websites, akademische Papers, Praxis-Literatur etc. → alle Quellen kurz in ein, zwei Sätzen zusammenfassen
4. **Persönliche Meinung:** Was war neu, was war schon bekannt, sagen was man selber dazu denkt, was man gut oder schlecht an aktuellen Entwicklungen und Technologien findet (nicht Begriffsdefinitionen etc.), danach sagen was überwiegt, die positiven oder negativen Seiten? eigene Position vs. die von anderen Menschen reflektieren → Abschnitt in der Ich-Form schreiben, bspw. „Ich bin der Überzeugung, dass Datenschutz gut ist für die Gesellschaft weil...“