# “Datenschutz Engineering”
## Warum Datenschutz auch ein technisches Problem ist

Viele der Vorträge haben einen Datenschutzaspekt ihrer Projekte erwähnt, nur wenige sind jedoch im Detail darauf eingegangen, ob ihre Projekte datenschutzkonform arbeiten, wie dies sichergestellt wird und welche Probleme insbesondere mit Inkrafttreten der **DSGVO** zu erwarten sind. Ich möchte zeigen, dass Datenschutz nicht nur ein rechtlicher Aspekt ist, sondern viele Projekte auch vor konkrete technische Herausforderungen stellen kann.

Die im Mai inkrafttretende EU-**Datenschutzgrundverordnung** „enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.“
Sie betrifft alle EU-Unternehmen und Unternehmen, die personenbezogene Daten über in der EU ansässige Personen erheben, verarbeiten und nutzen [..]. **Die maximale Geldbuße beträgt bis zu 20 Millionen Euro oder bis zu 4% des gesamten weltweit erzielten Jahresumsatzes.**

### Grundsätze der DSGVO
Nach Art. 5 DSGVO

Personenbezogene Daten müssen...

auf rechtmäßige Weise […] in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (**Transparenz**)

- Im November 2017 wurde bekannt, dass Android-Handys Ihren Standort auch dann an Google übermitteln, wenn die Standortdienste zuvor explizit deaktiviert wurden
- Googles Streetview-Autos schnitten 2008 bis 2010 im Vorbeifahren unverschlüsselten WLAN-Verkehr mit. In den USA wurde Google dafür zu einer Strafzahlung von 7 Millionen US-Dollar verurteilt

sachlich richtig [...] sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die [...] unrichtig sind, unverzüglich gelöscht oder berichtigt werden (**Richtigkeit**)

- 2008 berichtete Stiftung Warentest, dass durch irreführendes UI bei Banken häufig eine falsche Auskunft an die Schufa übermittelt wird, die zu einem schlechteren Rating führen kann. Die Kunden bekommen davon oft nichts mit und sind für eine Korrektur auf die Kooperation der Bank angewiesen.

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

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 (**Speicherbegrenzung**)

- Wie von Lennart Heuckendorf in der RingVL eindrucksvoll am Beispiel der Australischen Vorratsdatenspeichrung präsentiert, können selbst die anonymisierten Metadaten eines Mobiltelefons die eindeutige Identifizierung von Personen erlauben
- Michael Hayden (Früherer Direktor der NSA): „We kill people based on metadata“
- Auch in Deutschland gibt es eine anlasslose Vorratsdatenspeicherung

dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (**Datenminimierung**)

- Das deutsche Bundedatenschutzgesetz nennt die Prinzipien der Datenvermeidung und der Datensparsamkeit. Der Begriff „Datenminimierung“ enthält diese Prinzipien bereits

in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet (**Integrität und Vertraulichkeit**)

- 2014 wurden bei Yahoo mindestens 500 Millionen Accountdaten entwendet, teilweise inklusive Telefonnummern, Geburtsdaten, Sicherheitsfragen und Passwörtern.
- 2017 wurde bekannt, dass die Social Security Numbers von 143 Millionen US-Steuerzahlern bei der Firma Equifax entwendet wurden

### Lennart Heuckendorf
### The science behind visual analytics

„Basierend auf Metadaten könnten wir genau das Gebäude herausfinden, in dem der Journalist Will Ockenden wohnt.“

Anonymisierte Metadaten können also durchaus personenbezogene Daten beinhalten und fallen damit ggf. unter die DSGVO. Wie und ob Informationen wirksam anonymisiert werden können, um daraus keine Rückschlüsse mehr auf personenbezogene Daten ziehen zu können, ist zu diskutieren und zu erforschen.

### Dr. Matthias Weidlich
### Queue Mining

„Each and every patient at Dana-Farber Institute carries a badge, so you can see their position live on this screen. Imagine this in Europe! Being in the US makes some aspects of data handling easier.“

Ein solches Szenario ist in der EU tatsächlich schwer vorstellbar. Das Prinzip der Transparenz kann vielleicht eingehalten werden. Alle anderen Prinzipien der DSGVO dürften nur schwer zu garantieren sein. Insbesondere bei Vertraulichkeit, Zweckbindung, Datenminimierung und Speicherbegrenzung sehe ich hier aufkommende technische Herausforderungen. Absolute IT-Sicherheit zum Zwecke der Vertraulichkeit ist nach wie vor kein gelöstes Problem, Zweckbindung sicherzustellen erfordert Access Controls einer Art, die mir bisher nicht bekannt ist. Um Datenminimierung und Speicherbegrenzung zu ermöglichen, müsste es regelmäßig ablaufende Routinen geben, die autonom Daten klassifizieren und sie ggf. sofort auf sichere Weise löschen. Hinzu kommt, dass Gesundheitsdaten in der EU ein besonderes Schutzniveau haben, das über das von normalen personenbezogenen Daten hinaus geht.

**Hagen Echzell**

Ringvorlesung Data Engineering in der Praxis
Masterstudiengang „IT-Systems Engineering“
Hasso Plattner Institut, Potsdam

E-Mail: hagen.echzell@student.hpi.de